



US011868504B2

(12) **United States Patent**
Farchy et al.

(10) **Patent No.: US 11,868,504 B2**
(45) **Date of Patent: Jan. 9, 2024**

(54) **OWNERSHIP DETERMINATION IN
PRIVACY FIREWALLS**

(71) Applicant: **LYNX MD LTD.**, Tel Aviv (IL)

(72) Inventors: **Ofir Farchy**, Modiin (IL); **Omer Dror**,
Tel Aviv (IL)

(*) Notice: Subject to any disclaimer, the term of this
patent is extended or adjusted under 35
U.S.C. 154(b) by 425 days.

(21) Appl. No.: **17/126,234**

(22) Filed: **Dec. 18, 2020**

(65) **Prior Publication Data**
US 2021/0133351 A1 May 6, 2021

(58) **Field of Classification Search**
CPC G06F 21/6245; G06F 16/24568; G06F
16/2358; G06F 2221/2145; G06N 20/00
USPC 726/27
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

10,535,020 B2 * 1/2020 Experton G06Q 10/06
10,628,058 B1 * 4/2020 Riley G06F 3/067
(Continued)

FOREIGN PATENT DOCUMENTS

CN 110555072 A * 12/2019

OTHER PUBLICATIONS

Deborah J. Primary Care Practices' Abilities And Challenges In
Using Electronic Health Record Data For Quality Improvement;
Healthaffir; 2016; pp. 635-643.*

Primary Examiner — Monjur Rahim
(74) *Attorney, Agent, or Firm* — The Roy Gross Law
Firm, LLC; Roy Gross

Related U.S. Application Data

(60) Provisional application No. 62/950,188, filed on Dec.
19, 2019, provisional application No. 63/026,154,
filed on May 18, 2020.

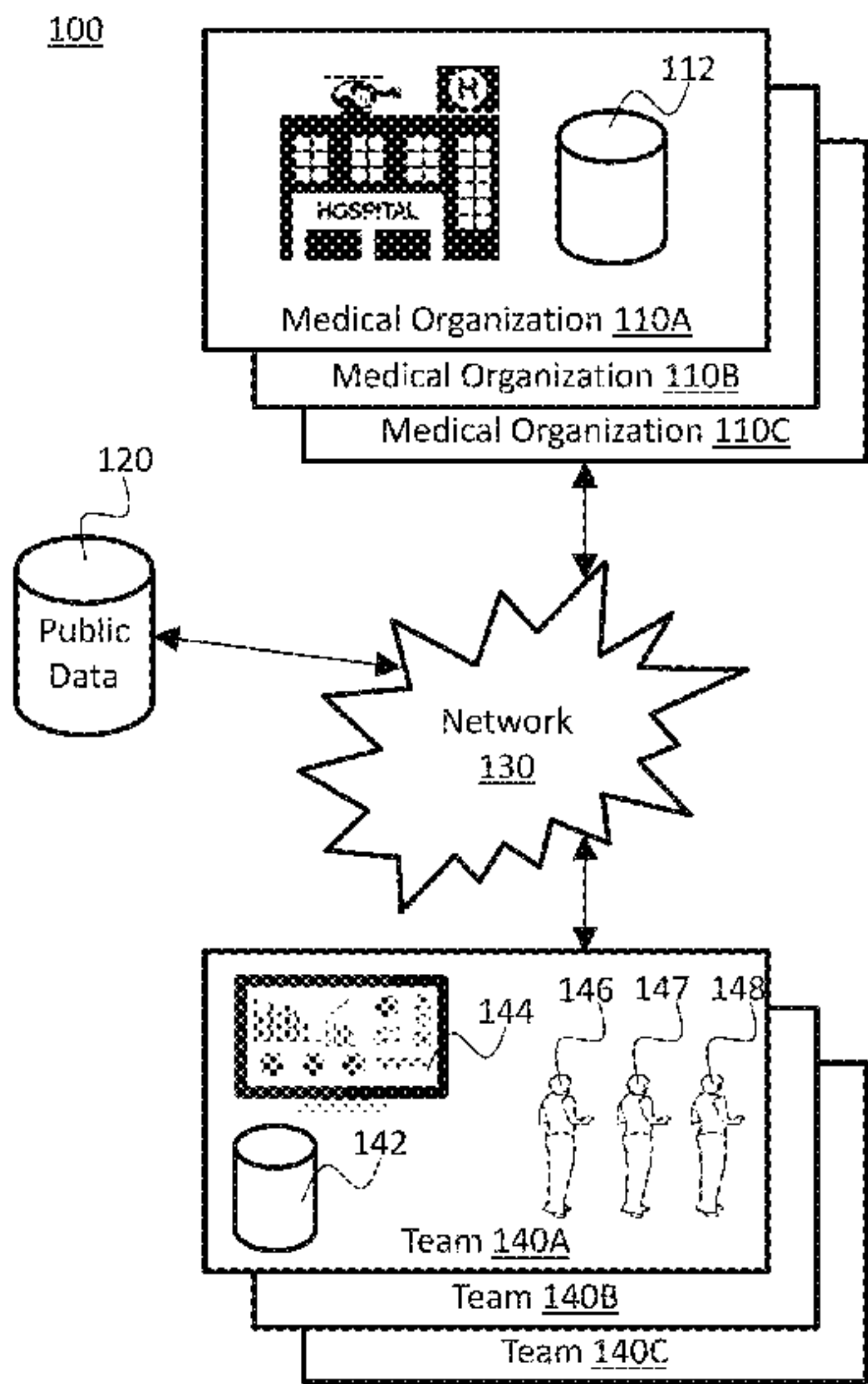
(51) **Int. Cl.**
G06F 16/23 (2019.01)
G06F 21/62 (2013.01)
G06F 21/60 (2013.01)
H04L 9/40 (2022.01)
G16H 10/60 (2018.01)
G06F 16/2455 (2019.01)
G06N 20/00 (2019.01)
H04W 12/02 (2009.01)

(52) **U.S. Cl.**
CPC **G06F 21/6245** (2013.01); **G06F 16/2358**
(2019.01); **G06F 16/24568** (2019.01); **G06F**
21/606 (2013.01); **G06F 21/629** (2013.01);
G06N 20/00 (2019.01); **G16H 10/60**
(2018.01); **G06F 2221/2145** (2013.01); **H04W**
12/02 (2013.01)

(57) **ABSTRACT**

Systems, methods and non-transitory computer readable
media for ownership determination in privacy firewalls are
provided. A request of a user to perform an action for
creating a new data collection using source data collections
may be received. In response to the user not having permis-
sion to view at least part of at least one of the source data
collections and the user not being an owner of the at least
one of the source data collections, it may be determined that
the user is not an owner of the new data collection, and in
response to the user being at least an owner of the data
collection or having permission to view the entire data
collection for all source data collections, it may be deter-
mined that the user is an owner of the new data collection.

19 Claims, 21 Drawing Sheets



(56)

References Cited

U.S. PATENT DOCUMENTS

2008/0040151	A1 *	2/2008	Moore	G16H 40/67 705/2
2012/0232929	A1 *	9/2012	Experton	G16H 40/67 705/3
2013/0218829	A1 *	8/2013	Martinez	G06Q 10/10 707/608
2013/0291060	A1 *	10/2013	Moore	G06F 16/83 726/1
2014/0207686	A1 *	7/2014	Experton	G16H 80/00 705/51
2014/0278762	A1 *	9/2014	Noyes	G06Q 30/08 705/7.29
2016/0004820	A1 *	1/2016	Moore	G16H 15/00 705/3
2016/0103963	A1 *	4/2016	Mishra	G16H 10/65 705/3
2017/0068785	A1 *	3/2017	Experton	H04W 12/02
2018/0233225	A1 *	8/2018	Experton	G16H 50/50
2018/0336362	A1 *	11/2018	Guttmann	G06F 21/6218
2019/0087603	A1 *	3/2019	Dror	G06F 21/6245
2020/0134217	A1 *	4/2020	Vishnyakov	G06F 16/2456

* cited by examiner

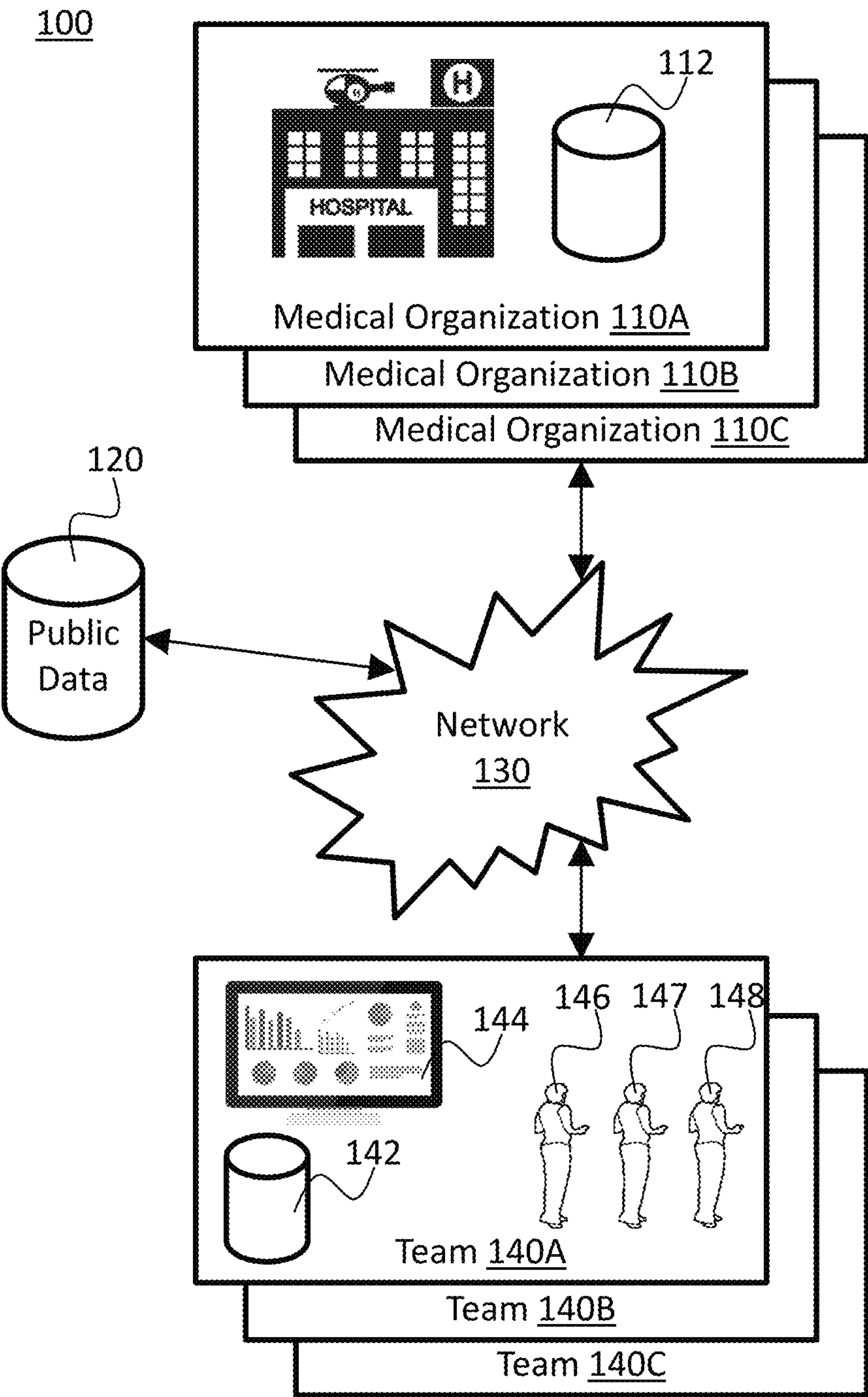


FIG. 1

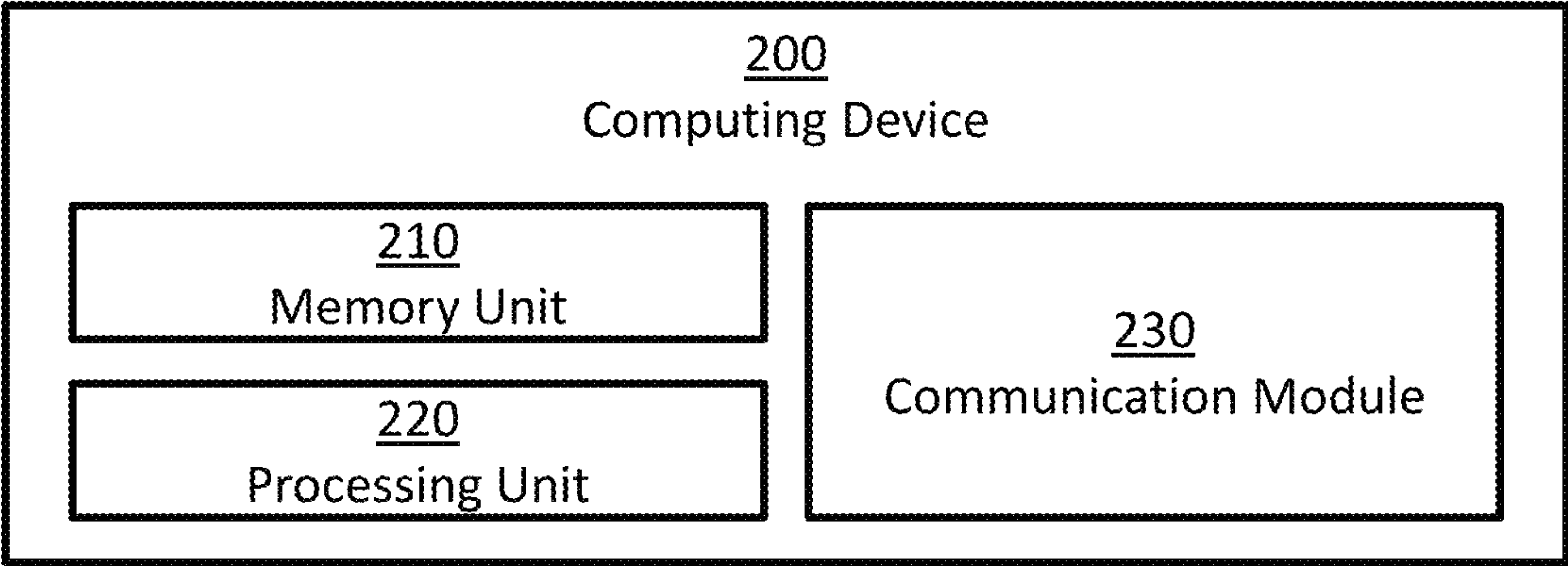


FIG. 2A

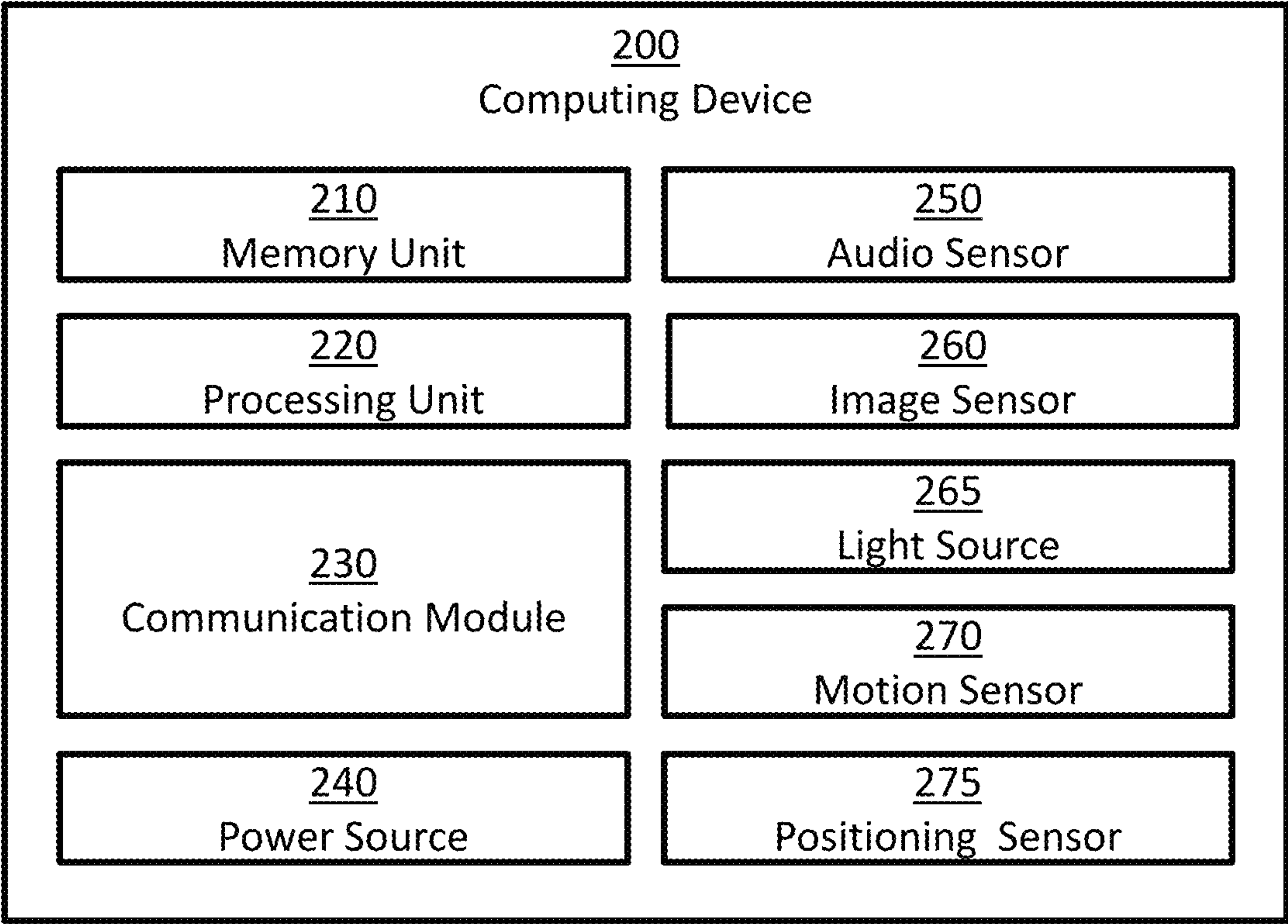


FIG. 2B

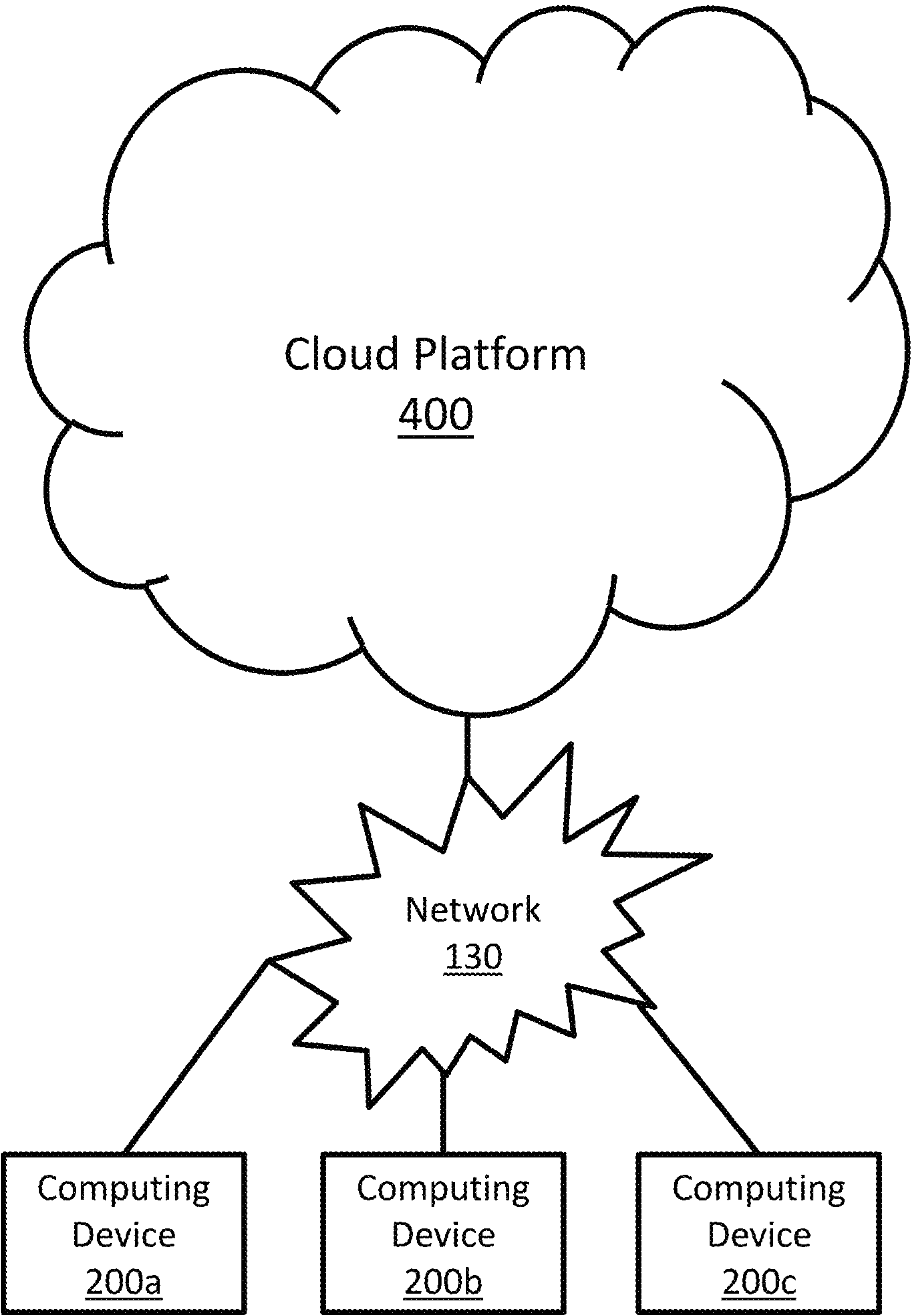


FIG. 3

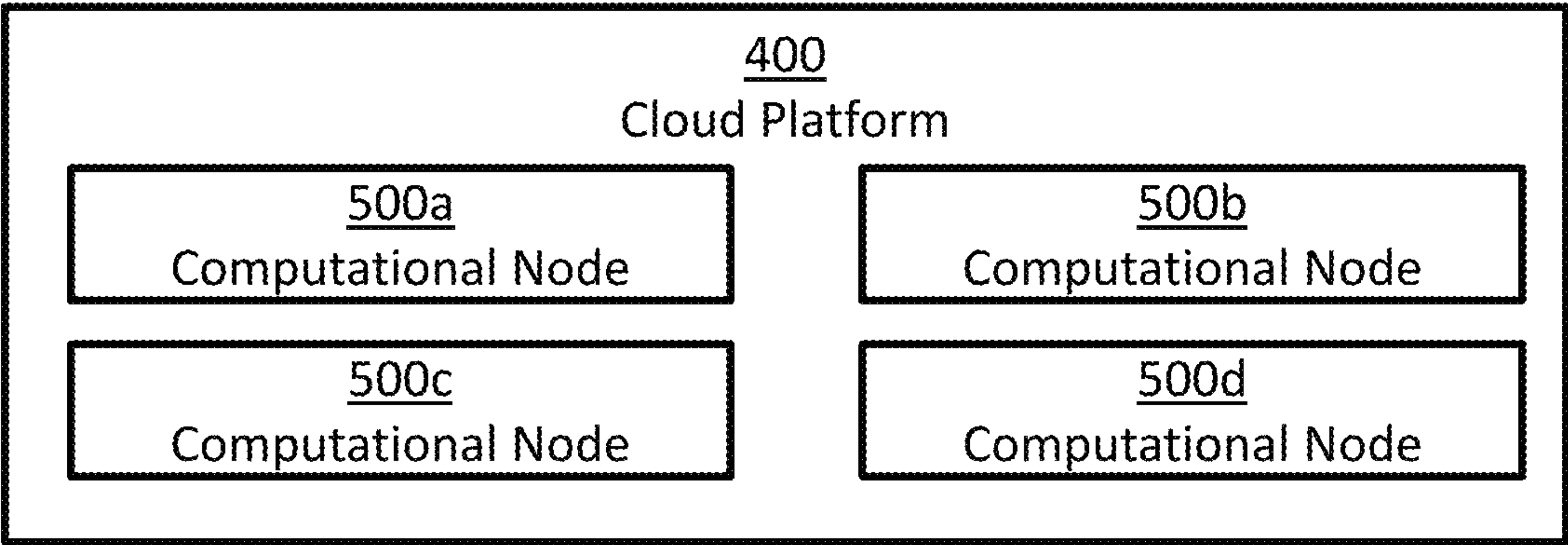


FIG. 4A

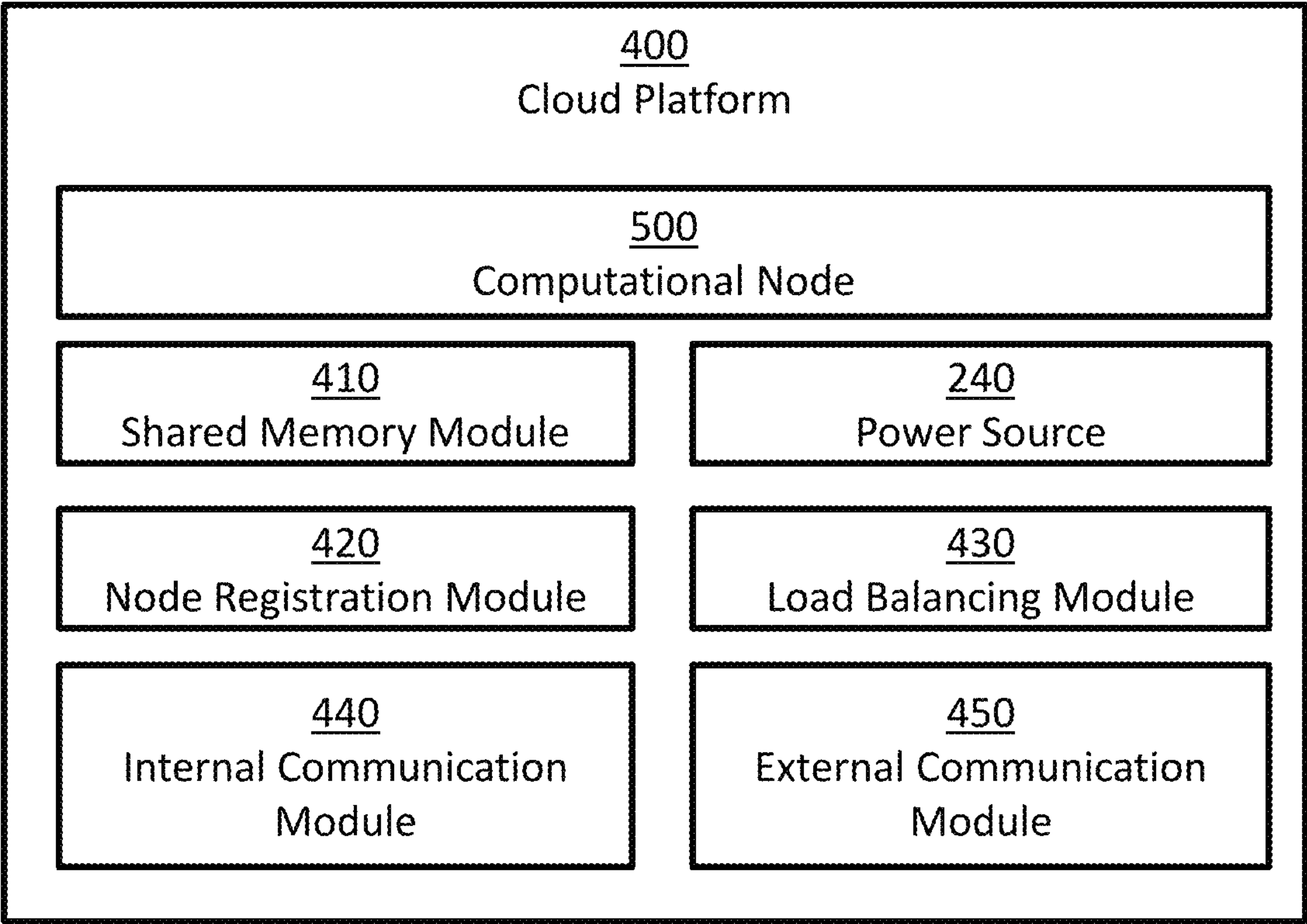


FIG. 4B

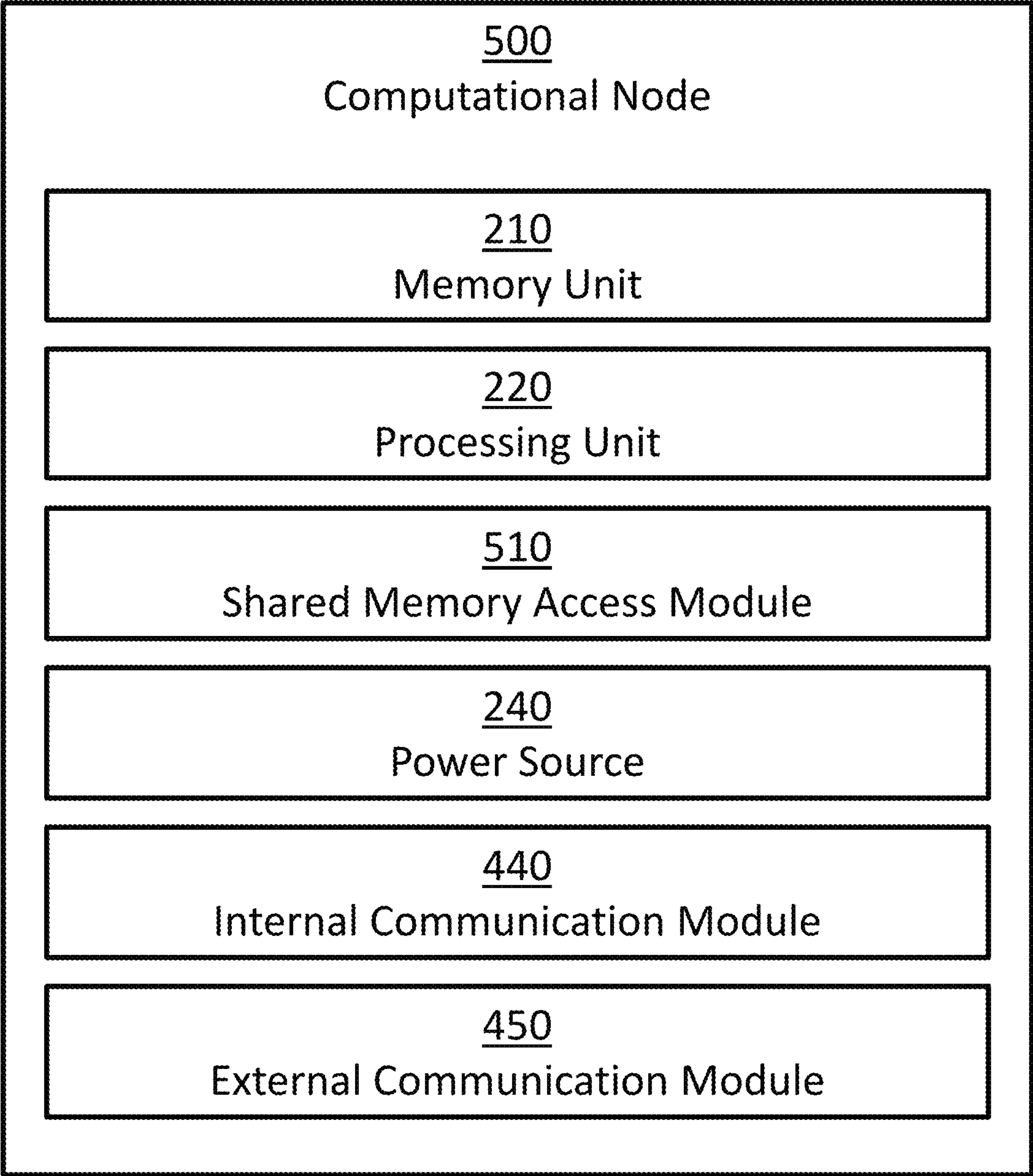


FIG. 5

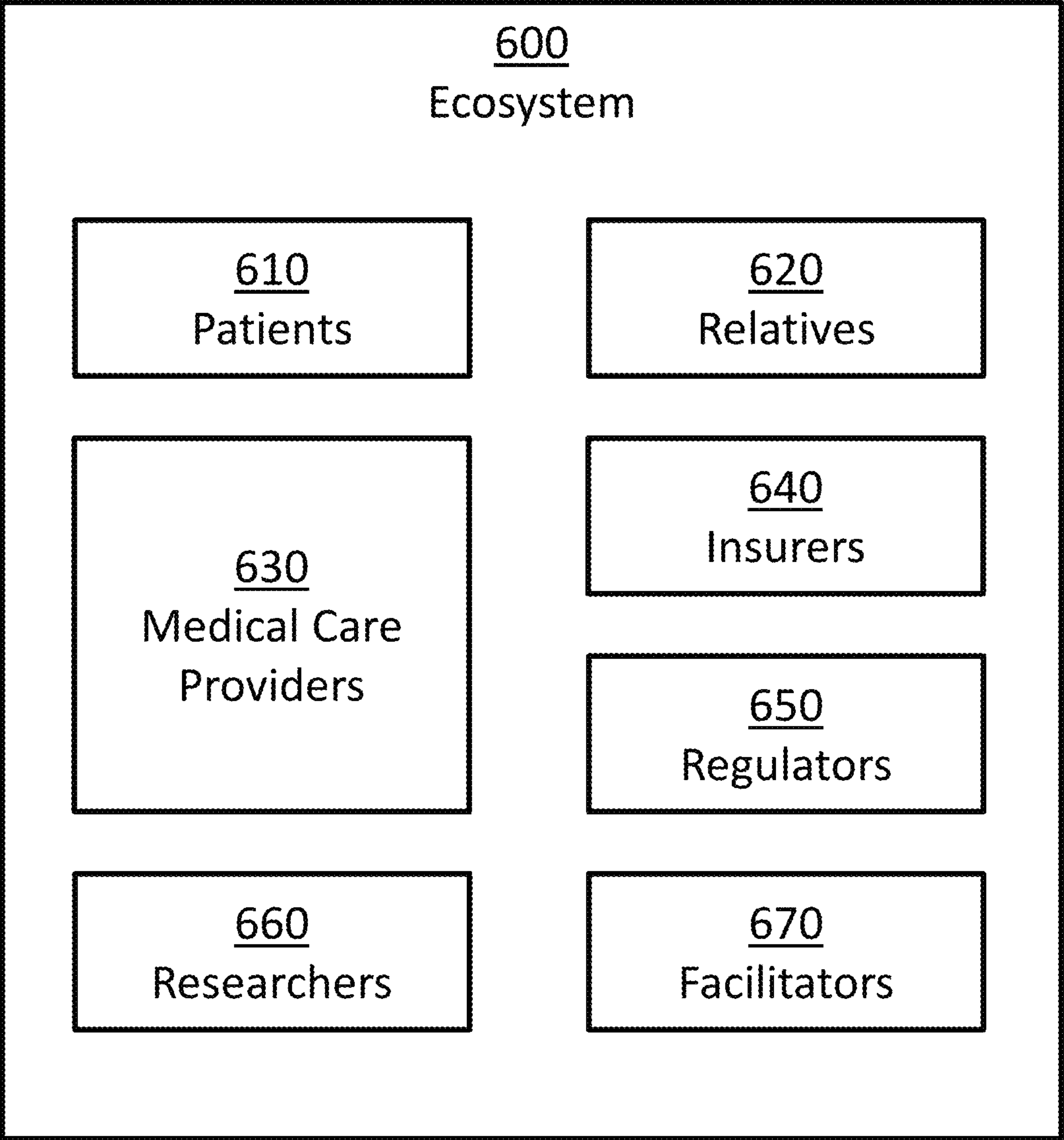


FIG. 6

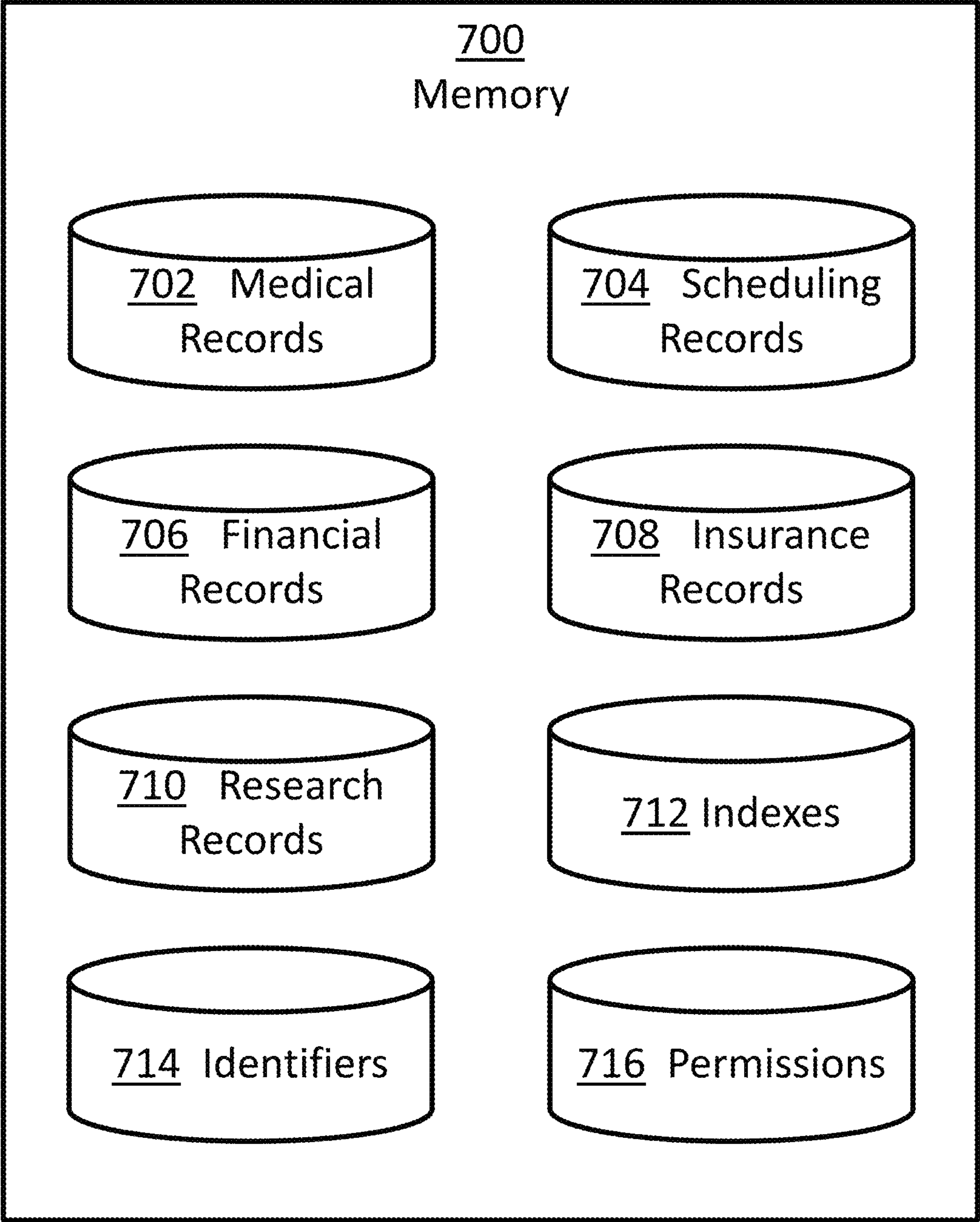


FIG. 7A

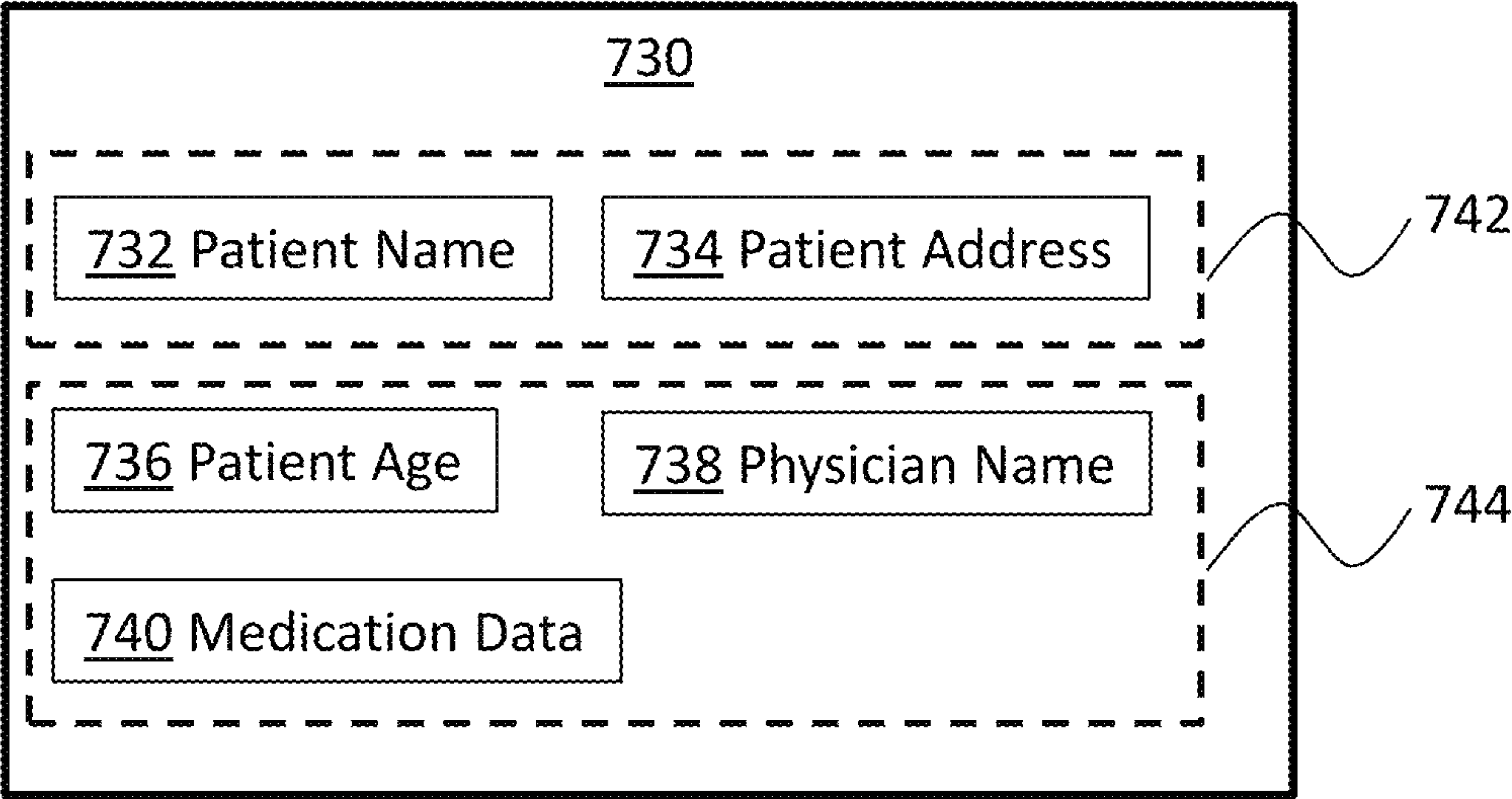


FIG. 7B

750

752 Patient Name	754 Patient Phone Number	756 Physician Name	758 Appointment Time
Mary Smith	555-####	James Miller	Dec. 16, 10:50
John Brown	555-####	Linda Jones	Dec. 16, 9:10

FIG. 7C

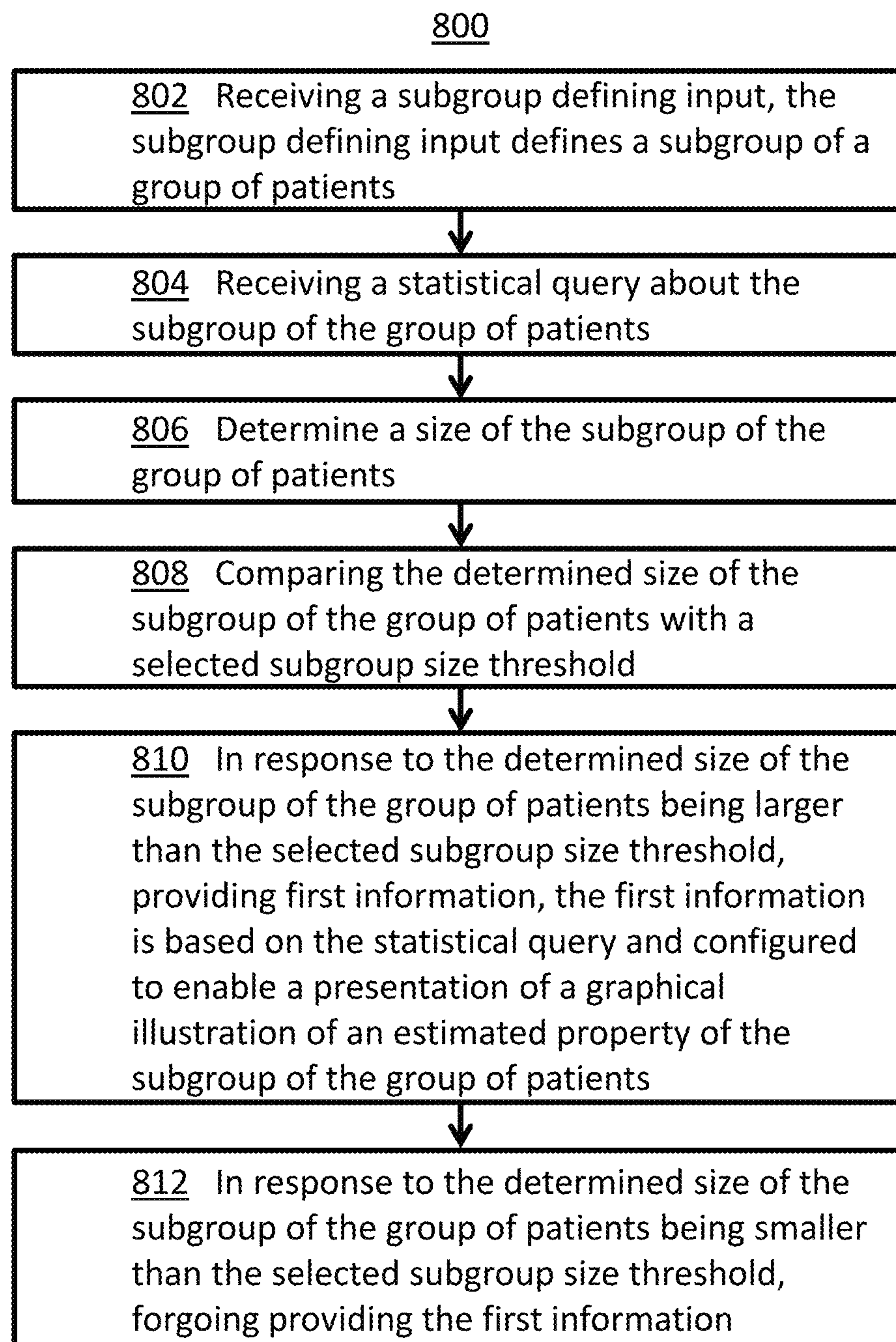
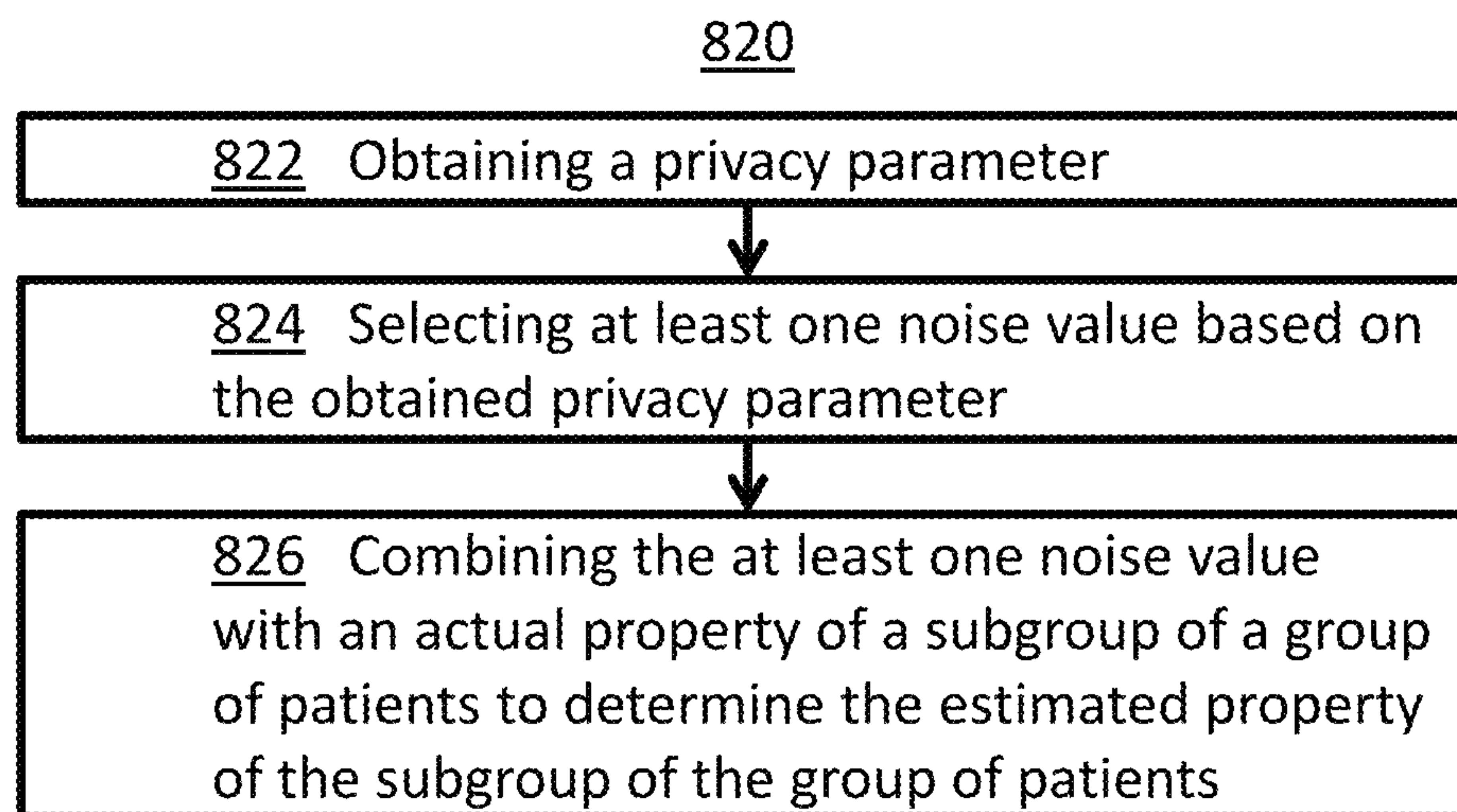
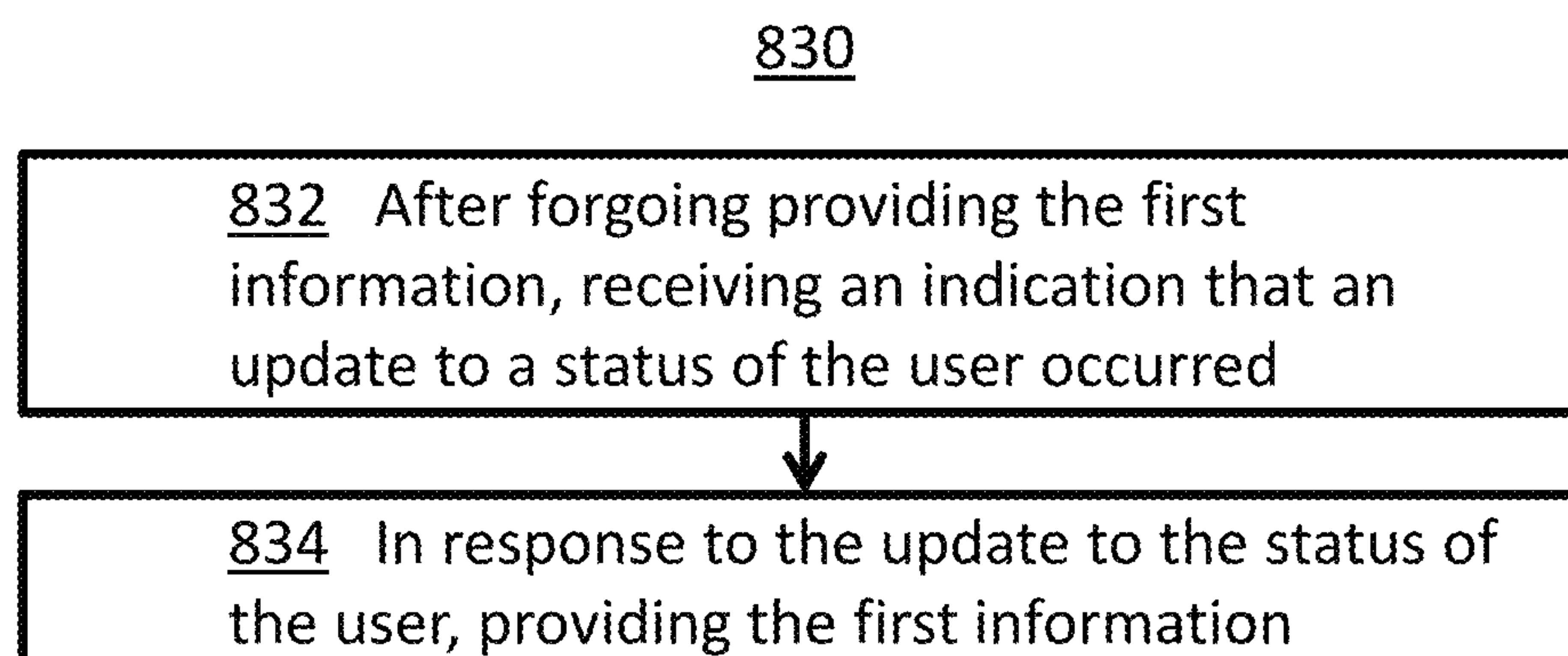
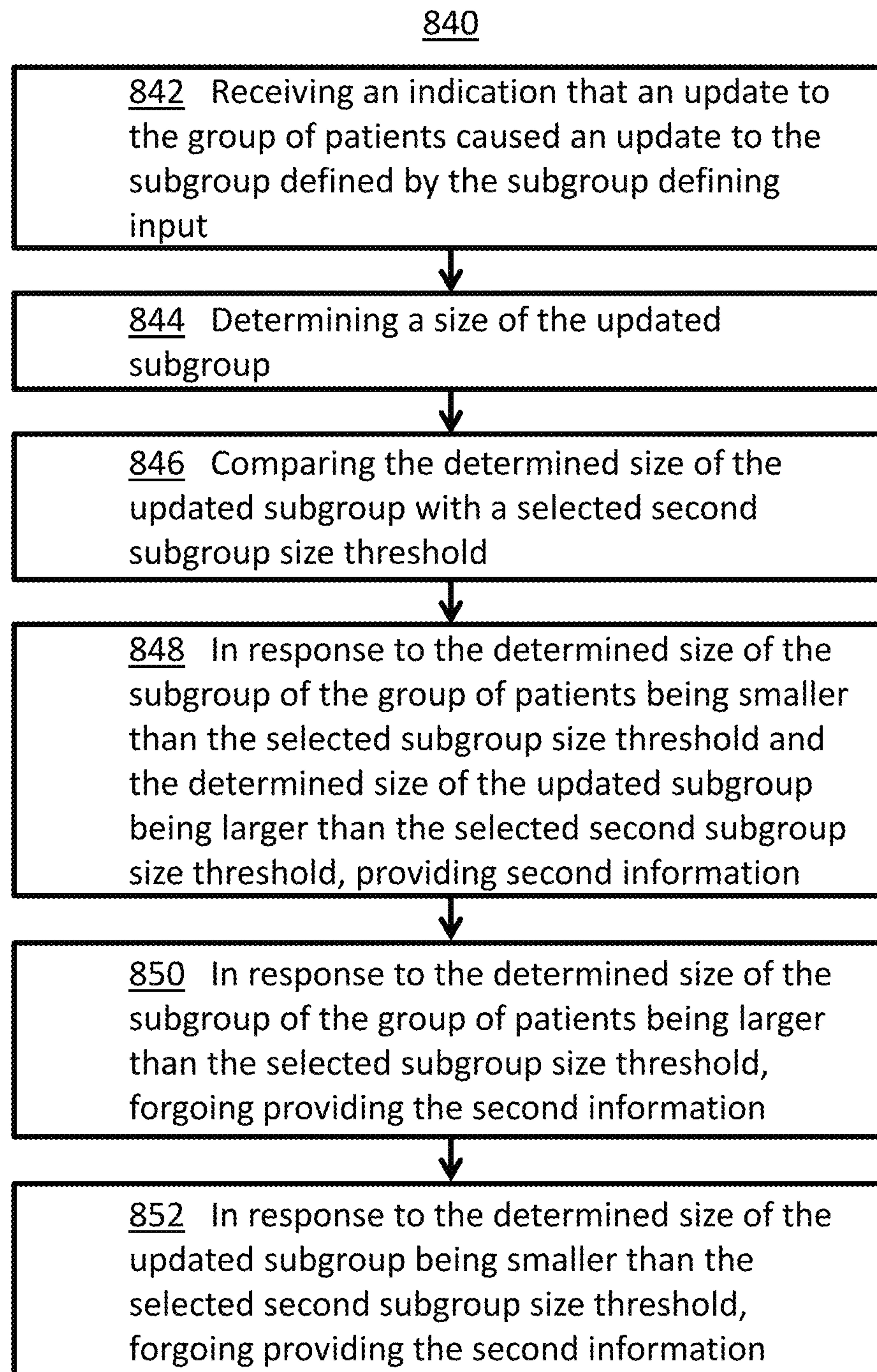


FIG. 8A

**FIG. 8B****FIG. 8C**

**FIG. 8D**

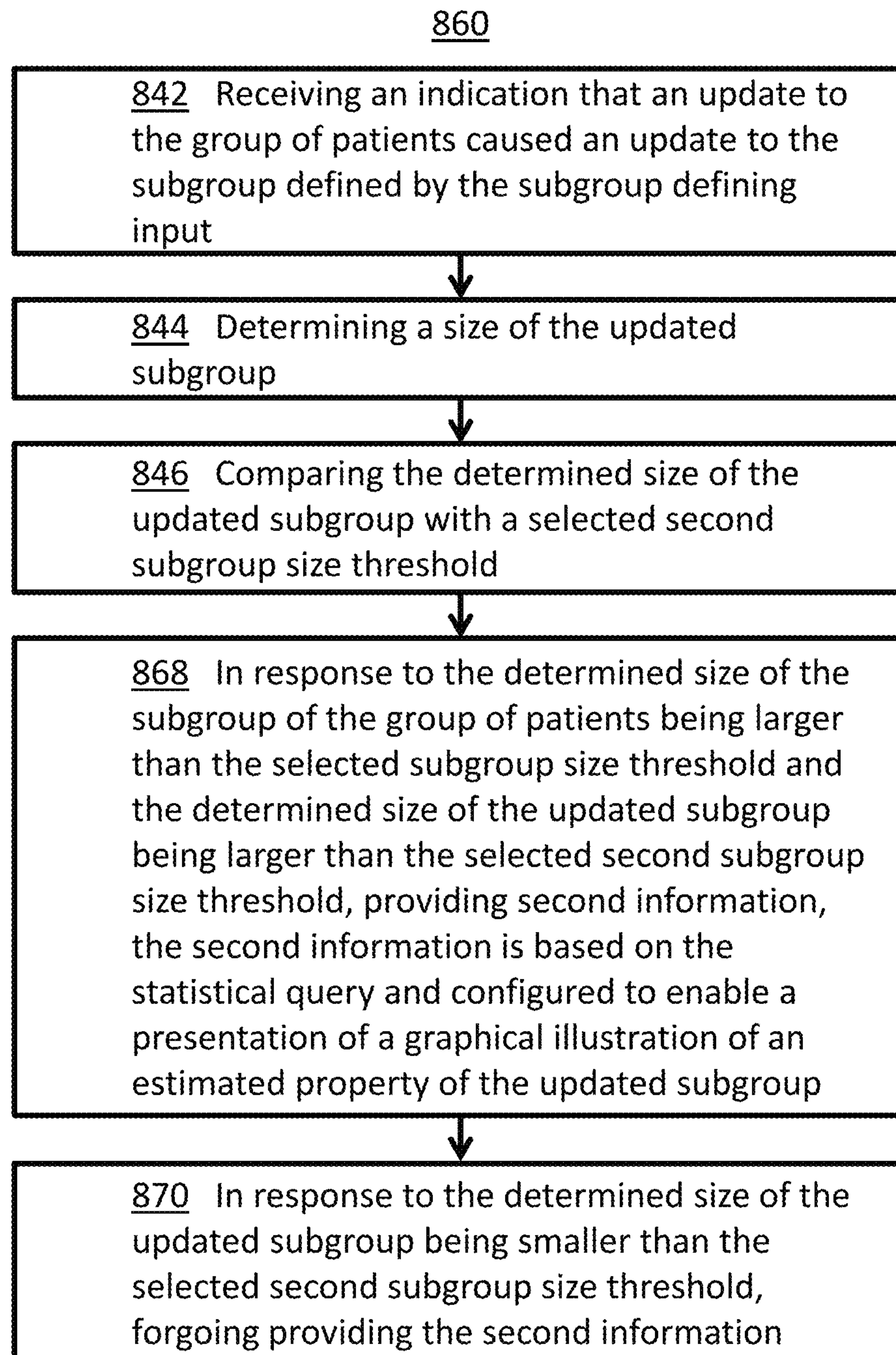


FIG. 8E

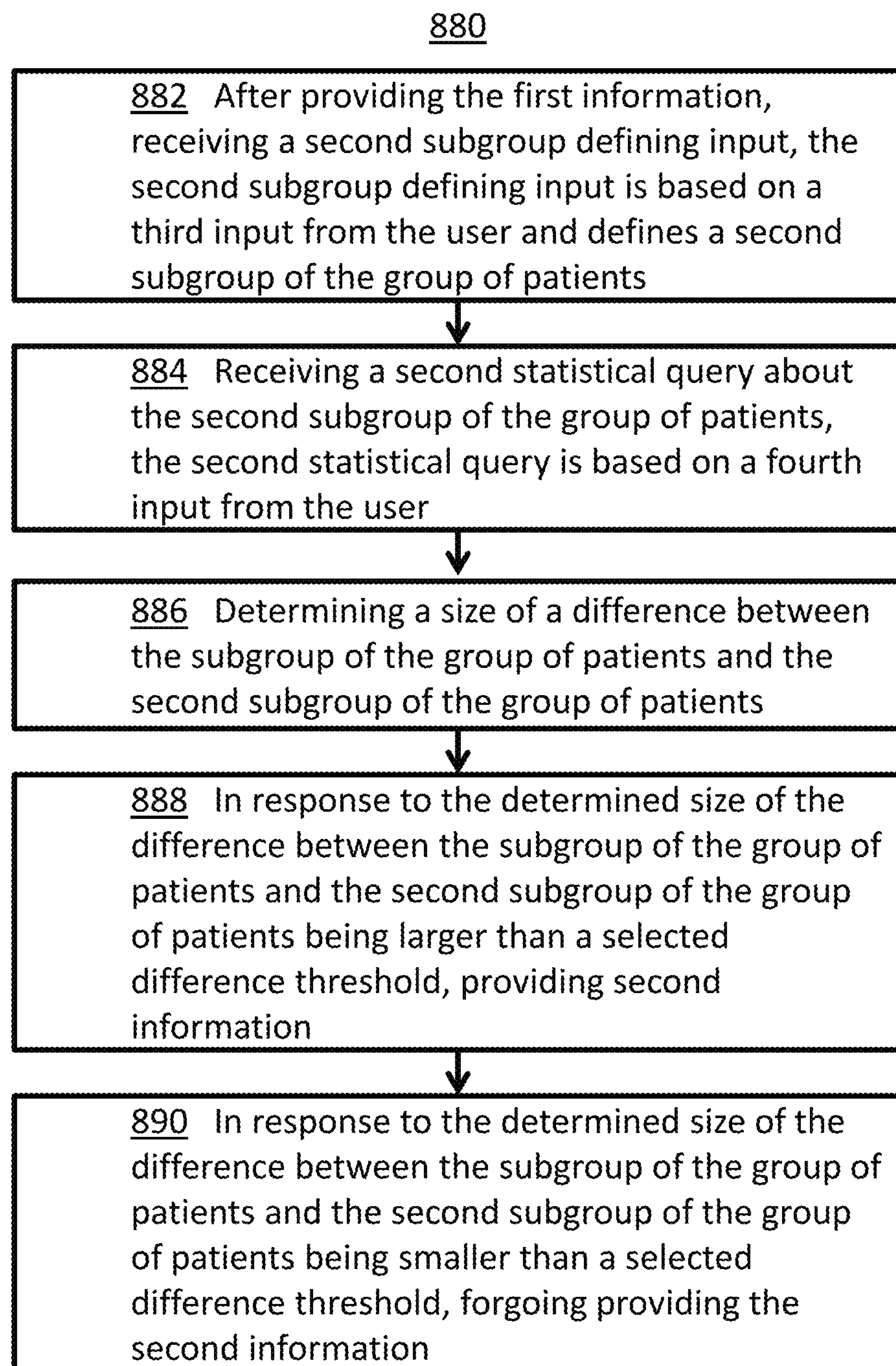


FIG. 8F

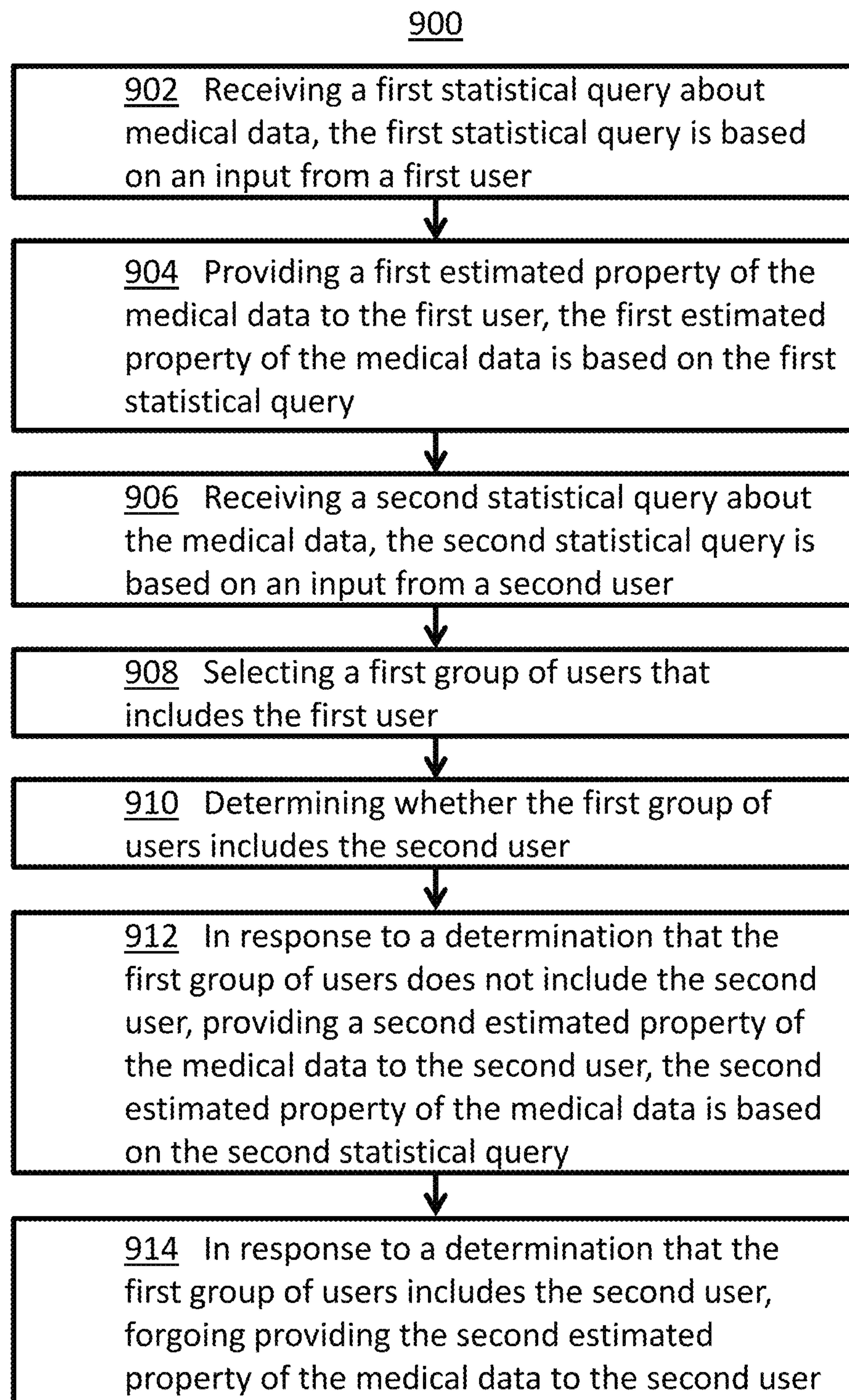
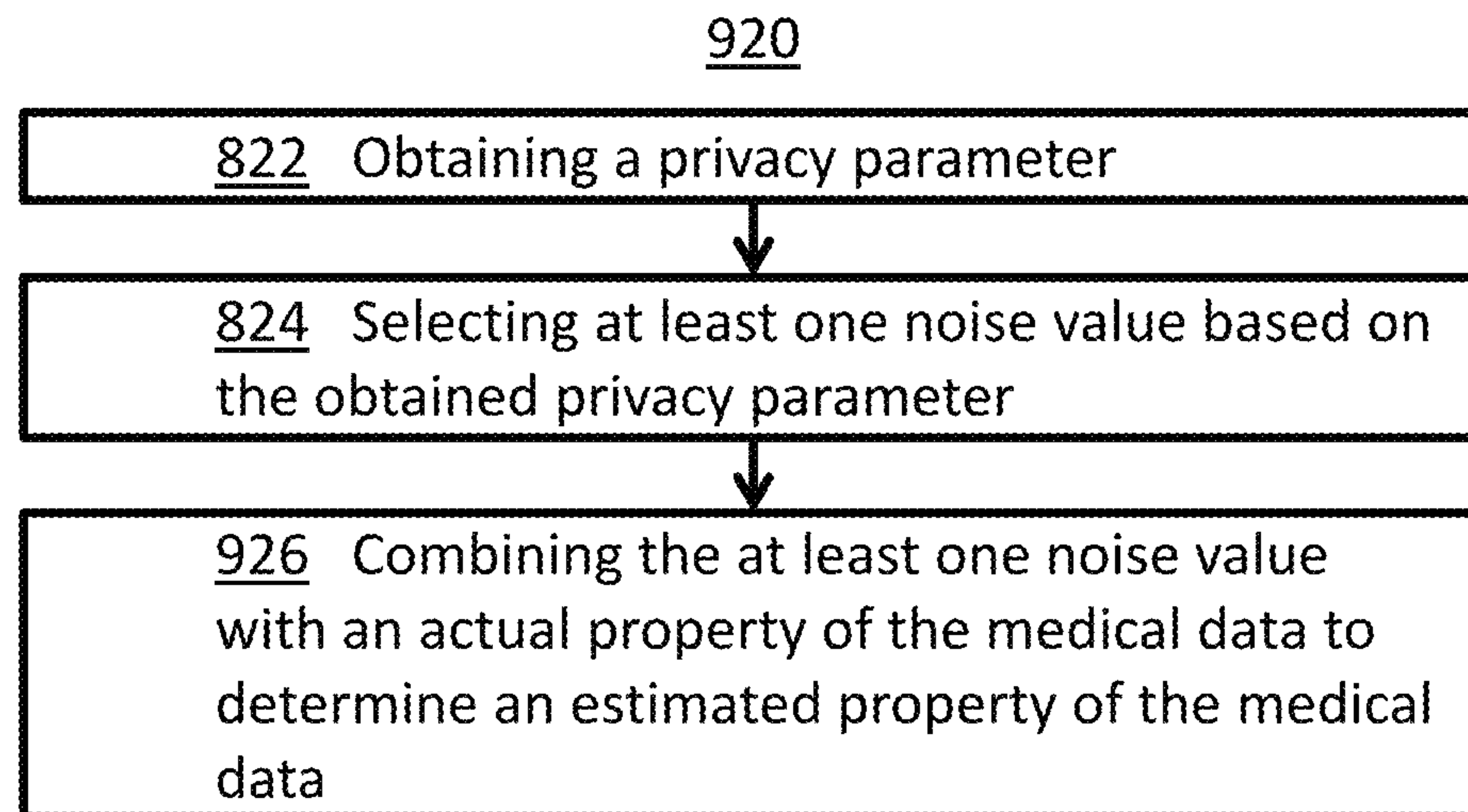
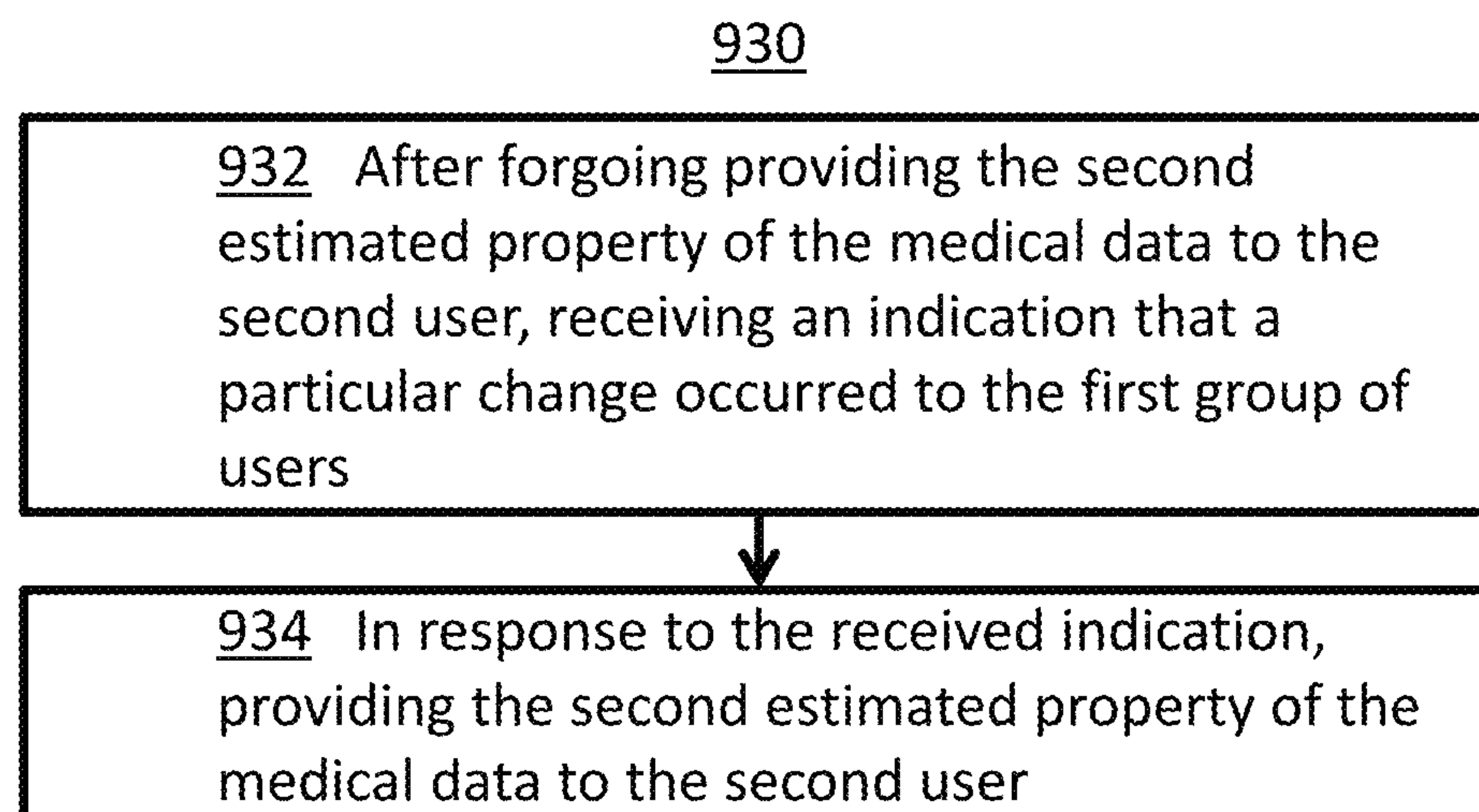
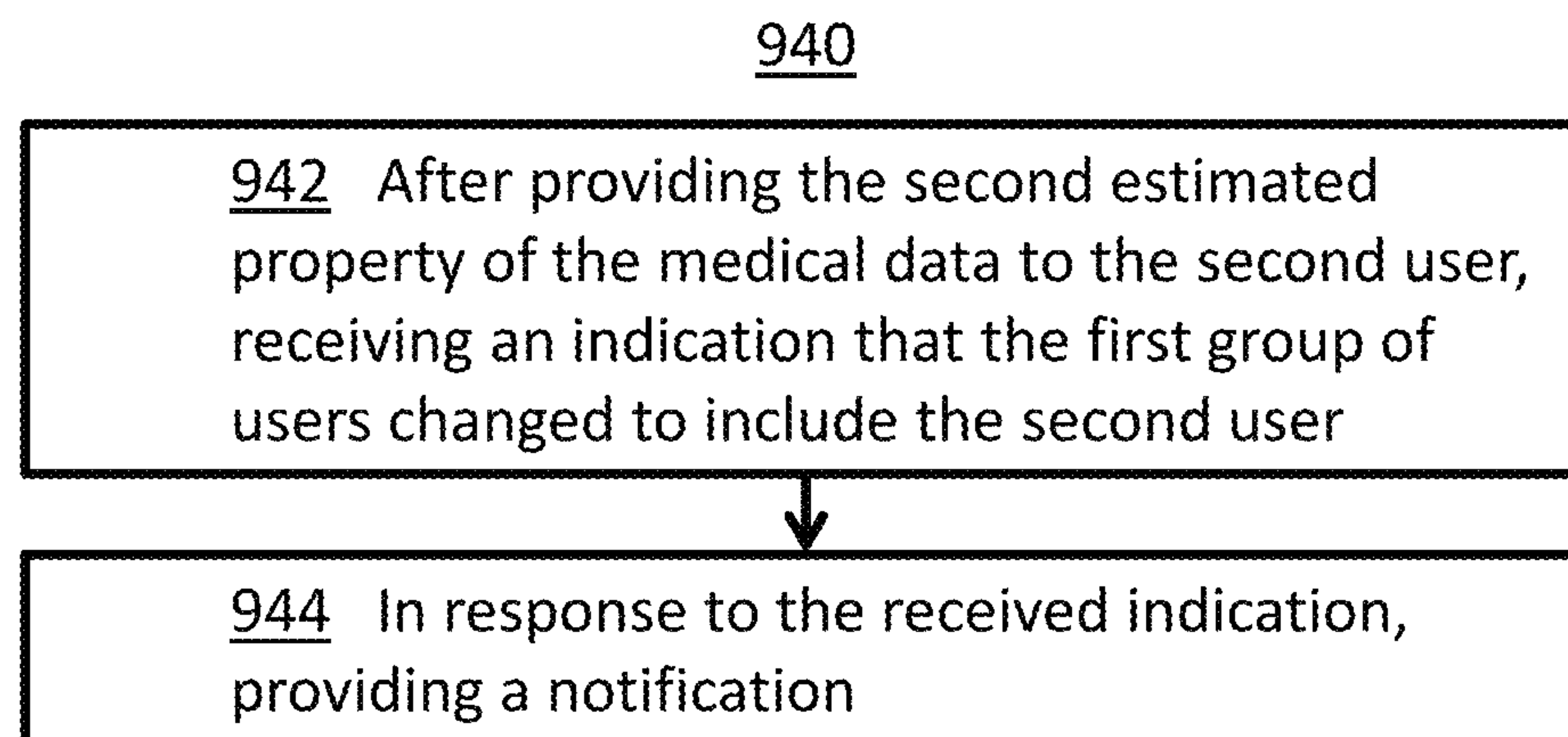
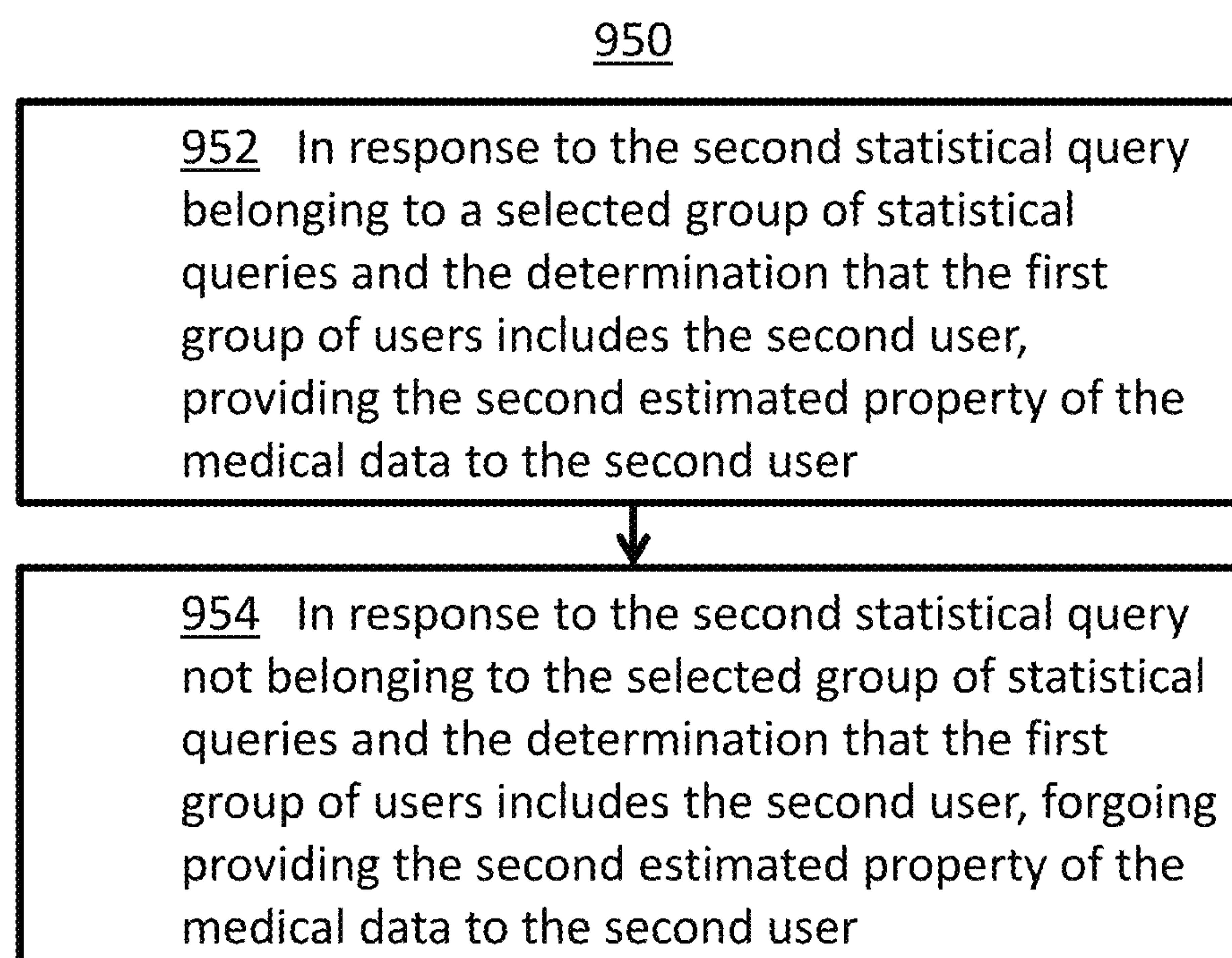


FIG. 9A

**FIG. 9B****FIG. 9C**

**FIG. 9D****FIG. 9E**

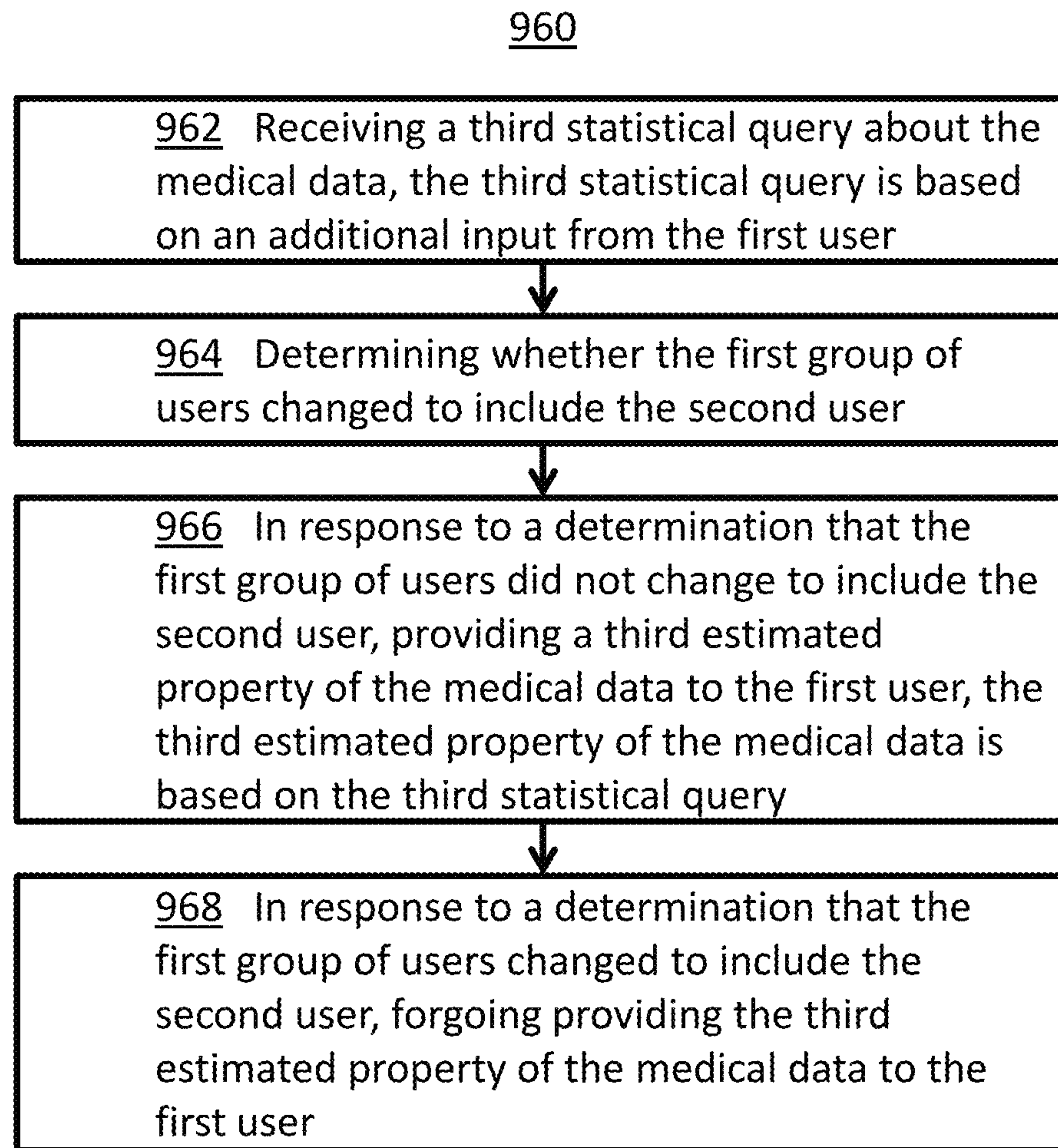


FIG. 9F

1000

1002 Receiving a request to access a content of an element, the content of the element includes at least a first portion and a second portion, the first portion includes identifiable information and the second portion does not include identifiable information



1004 Accessing a permission record corresponding to the element

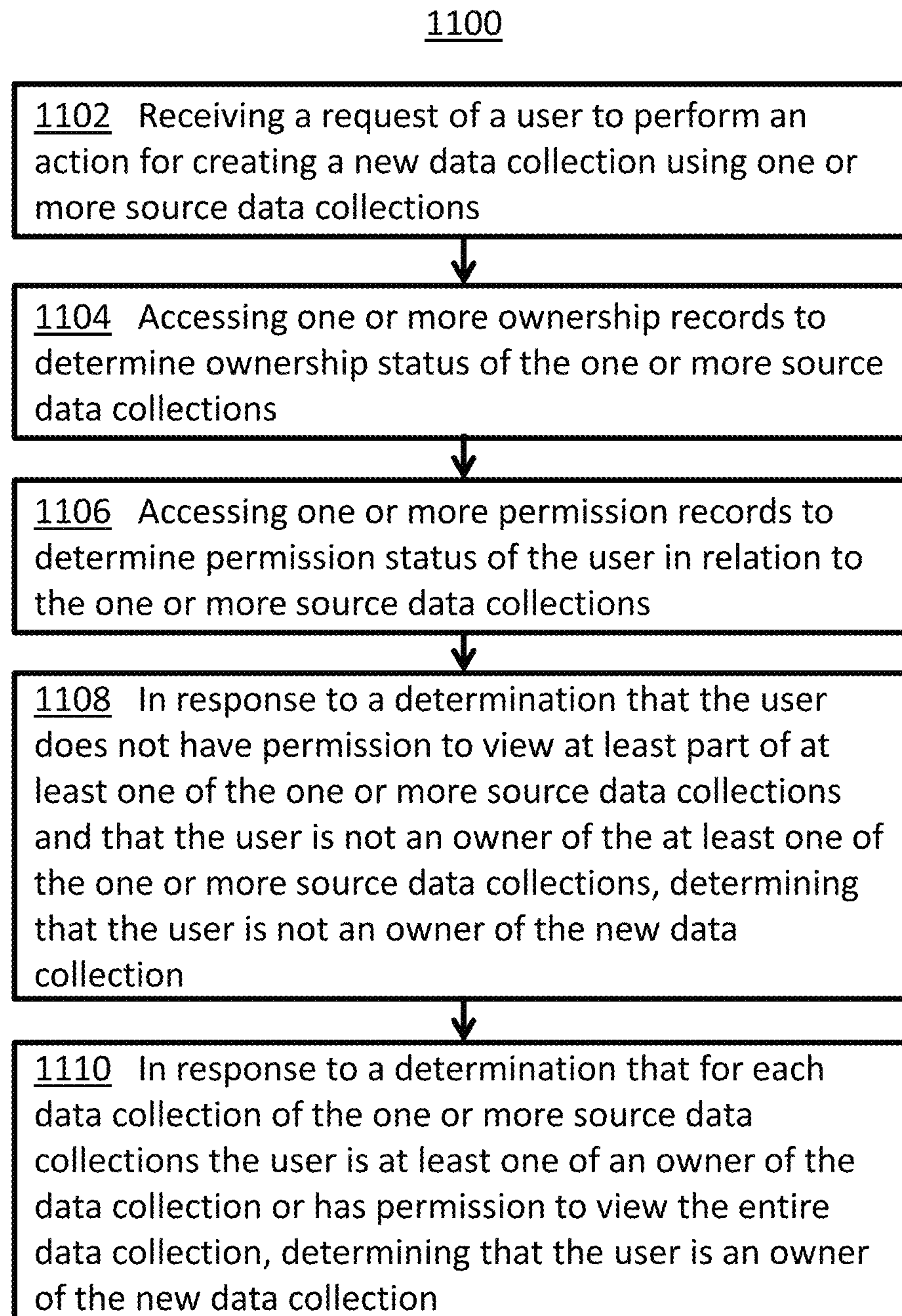


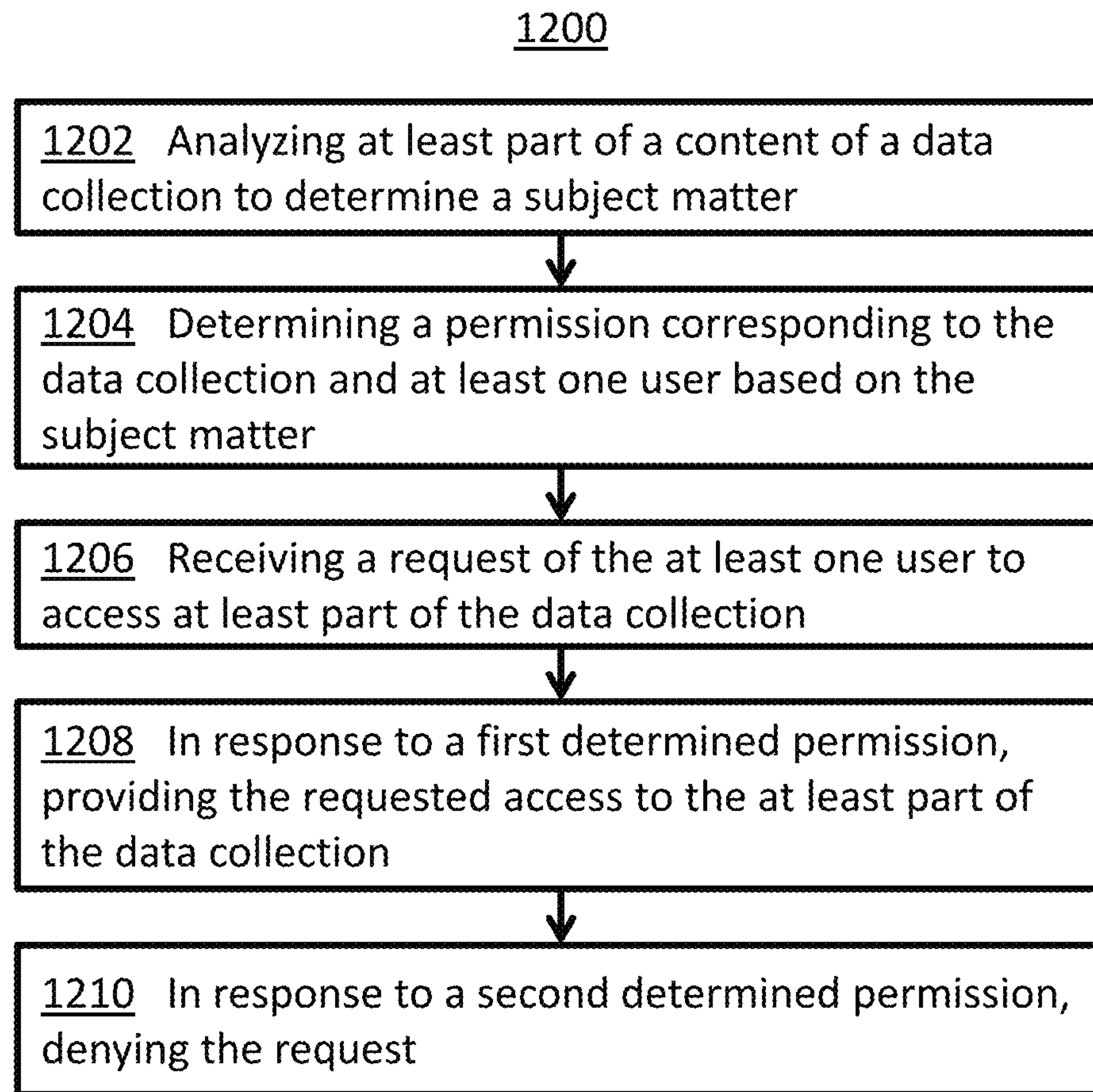
1006 In response to a first value in the permission record, providing access to the content of the element, including access to the first portion and the second portion of the content of the element

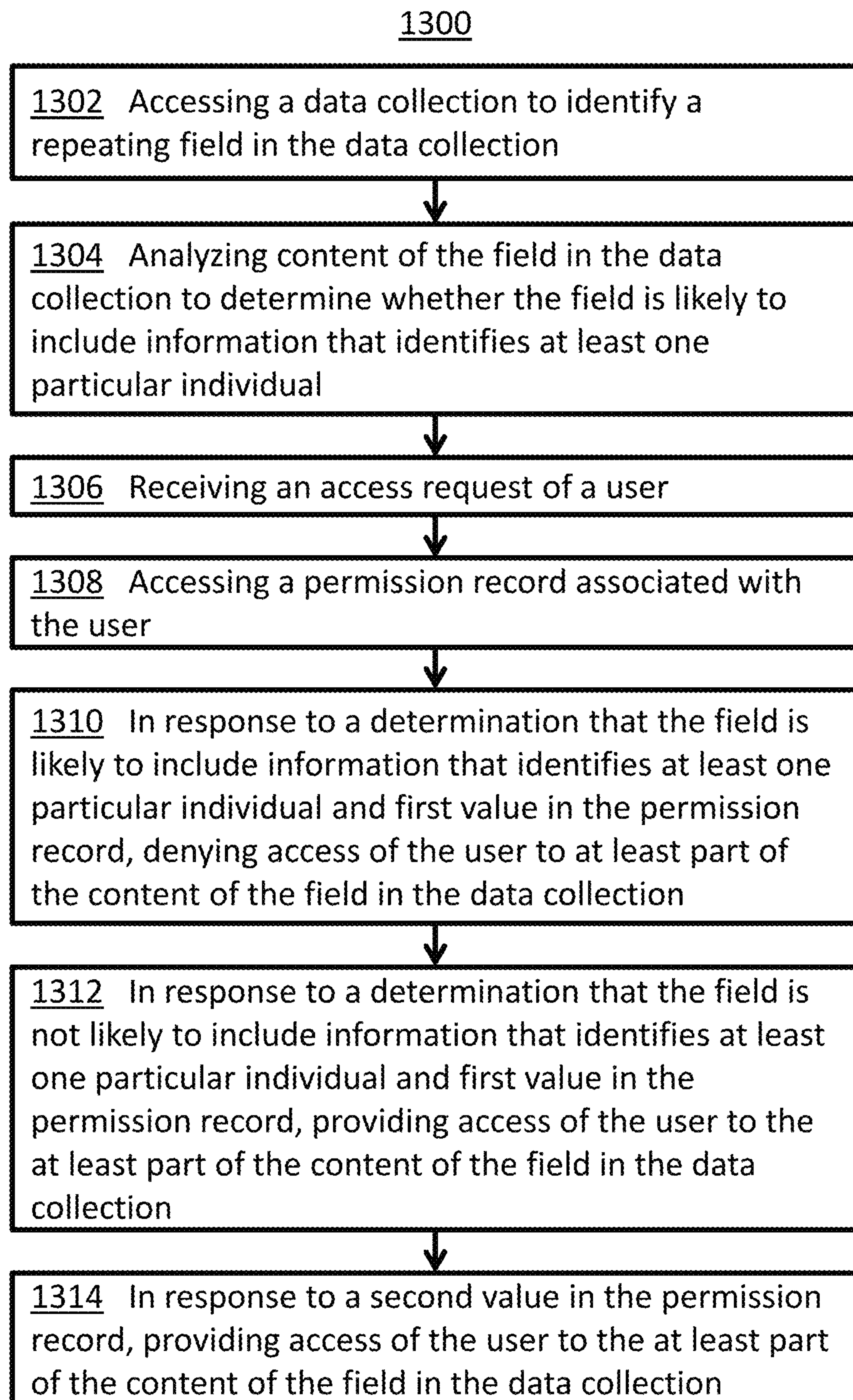


1008 In response to a second value in the permission record, providing partial access to the content of the element, the partial access includes access to the second portion of the content of the element and excludes access to the first portion of the content of the element

FIG. 10

**FIG. 11**

**FIG. 12**

**FIG. 13**

OWNERSHIP DETERMINATION IN PRIVACY FIREWALLS

CROSS REFERENCES TO RELATED APPLICATIONS

This application claims the benefit of priority of U.S. Provisional Patent Application No. 62/950,188, filed on Dec. 19, 2019, and U.S. Provisional Patent Application No. 63/026,154, filed on May 18, 2020.

The entire contents of all of the above-identified applications are herein incorporated by reference.

BACKGROUND

Technological Field

The disclosed embodiments generally relate to systems and methods for determining ownership of new data collections. More particularly, the disclosed embodiments relate to systems and methods for determining ownership of new data collections based on ownership and permissions of source data collections used to create the new data collections.

Background Information

Numerous medical records are created, read and edited by vast number of medical care providers. Nowadays, some medical research requires access to large datasets of medical information. However, accessing medical data may prove challenging, partly due to regulatory and privacy requirements. Easing access to medical data may facilitate accelerated medical research.

SUMMARY

Embodiments consistent with the present disclosure provide systems, methods, and devices for providing information based on private medical data.

In some embodiments, systems, methods and non-transitory computer readable media for enabling graphical illustration of private medical information are provided. In some examples, a subgroup defining input may be received, the subgroup defining input may be based on a first input from a user and may define a subgroup of a group of patients. Further, in some examples, a statistical query about the subgroup of the group of patients may be received, the statistical query may be based on a second input from the user. Further, in some examples, a size of the subgroup of the group of patients may be determined. Further, in some examples, the determined size of the subgroup of the group of patients may be compared with a selected subgroup size threshold. Further, in some examples, first information may be provided. For example, the first information may be based on the statistical query and may be configured to enable a presentation of a graphical illustration of an estimated property of the subgroup of the group of patients in response to the second input from the user. In some examples, in response to the determined size of the subgroup of the group of patients being larger than the selected subgroup size threshold, the first information may be provided, and in response to the determined size of the subgroup of the group of patients being smaller than the selected subgroup size threshold, providing the first information may be withheld and/or forwent.

In some embodiments, systems, methods and non-transitory computer readable media for facilitating privacy pre-

serving joint medical research are provided. For example, systems and method for selectively providing information about medical data are provided.

In some examples, a first statistical query about medical data may be received, the first statistical query may be based on an input from a first user. Further, in some examples, a first estimated property of the medical data may be provided to the first user, the first estimated property of the medical data may be based on the first statistical query. Further, in some examples, a second statistical query about the medical data may be received, the second statistical query may be based on an input from a second user (the second user may differ from the first user). Further, in some examples, a first group of users that includes the first user may be selected. Further, in some examples, it may be determined whether the first group of users includes the second user. Further, in some examples, in response to a determination that the first group of users does not include the second user, a second estimated property of the medical data may be provided to the second user (the second estimated property of the medical data may be based on the second statistical query), and in response to a determination that the first group of users includes the second user, providing the second estimated property of the medical data to the second user may be withheld and/or forwent. In some examples, the first estimated property of the medical data may be a first actual property of the medical data. In some examples, the first group of users may be selected of a plurality of alternative groups of users based on an identity of the first user. In some examples, a type of the first user may be a particular type, and the selected first group of users may include all users of the particular type from a particular plurality of users.

In some embodiments, systems, methods and non-transitory computer readable media for controlling access to private medical information are provided.

In some examples, a request to access a content of an element may be received, the content of the element may include at least a first portion and a second portion, the first portion may include identifiable information and the second portion may include no identifiable information. A permission record corresponding to the element may be accessed. In response to a first value in the permission record, access to the content of the element may be provided, including access to the first portion and the second portion of the content of the element, and in response to a second value in the permission record, partial access to the content of the element may be provided, the partial access may include access to the second portion of the content of the element and may exclude access to the first portion of the content of the element.

In some embodiments, systems, methods and non-transitory computer readable media for ownership determination are provided.

In some examples, a request of a user to perform an action for creating a new data collection using one or more source data collections may be received. One or more ownership records may be accessed to determine ownership status of the one or more source data collections. One or more permission records may be accessed to determine permission status of the user in relation to the one or more source data collections. In response to a determination that the user does not have permission to view at least part of at least one of the one or more source data collections and that the user is not an owner of the at least one of the one or more source data collections, it may be determined that the user is not an owner of the new data collection, and in response to a determination that for each data collection of the one or

3

more source data collections the user is at least one of an owner of the data collection or has permission to view the entire data collection, it may be determined that the user is an owner of the new data collection.

In some embodiments, systems, methods and non-transitory computer readable media for determining permissions are provided.

In some examples, at least part of a content of a data collection may be analyzed to determine a subject matter. A permission corresponding to the data collection and at least one user may be determined based on the subject matter. A request of the at least one user may be received to access at least part of the data collection. In response to a first determined permission, the requested access to the at least part of the data collection may be provided, and in response to a second determined permission, the request may be denied.

In some embodiments, systems, methods and non-transitory computer readable media for detecting identified information are provided.

In some examples, a data collection may be accessed to identify a repeating field in the data collection. Content of the field in the data collection may be analyzed to determine whether the field is likely to include information that identifies at least one particular individual. An access request of a user may be received. A permission record associated with the user may be accessed. In response to a determination that the field is likely to include information that identifies at least one particular individual and a first value in the permission record, access of the user to at least part of the content of the field in the data collection may be denied, in response to a determination that the field is not likely to include information that identifies at least one particular individual and the first value in the permission record, access of the user to the at least part of the content of the field in the data collection may be provided, and in response to a second value in the permission record, access of the user to the at least part of the content of the field in the data collection may be provided.

Consistent with other disclosed embodiments, a non-transitory computer readable medium may store software programs, each software program comprising data and computer implementable instructions for carrying out any of the methods described herein. For example, when the software program is executed by at least one processing device, it may be configured to perform any of the methods described herein.

The foregoing general description and the following detailed description are exemplary and explanatory only and are not restrictive of the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is an illustration of an exemplary system for providing information based on medical data.

FIGS. 2A and 2B are block diagrams illustrating some possible implementations of a computing device.

FIG. 3 is a block diagram illustrating a possible implementation of a communicating system.

FIGS. 4A and 4B are block diagrams illustrating some possible implementations of a cloud platform.

FIG. 5 is a block diagram illustrating a possible implementation of a computational node.

FIG. 6 is a block diagrams illustrating a possible ecosystem.

FIG. 7A illustrates an exemplary embodiment of a memory storing a plurality of modules.

4

FIG. 7B illustrates an exemplary embodiment of a data element.

FIG. 7C illustrates an exemplary embodiment of a data element.

FIG. 8A illustrates an example of a method for enabling graphical illustration based on private medical information.

FIG. 8B illustrates an example of a method for determining an estimated property of a subgroup of a group of patients.

FIG. 8C illustrates an example of a method for enabling graphical illustration based on private medical information.

FIG. 8D illustrates an example of a method for enabling graphical illustration based on private medical information.

FIG. 8E illustrates an example of a method for enabling graphical illustration based on private medical information.

FIG. 8F illustrates an example of a method for enabling graphical illustration based on private medical information.

FIG. 9A illustrates an example of a method for selectively providing information about medical data.

FIG. 9B illustrates an example of a method for determining an estimated property of medical data.

FIG. 9C illustrates an example of a method for selectively providing information about medical data.

FIG. 9D illustrates an example of a method for selectively providing information about medical data.

FIG. 9E illustrates an example of a method for selectively providing information about medical data.

FIG. 9F illustrates an example of a method for selectively providing information about medical data.

FIG. 10 illustrates an example of a method for controlling access to private medical information.

FIG. 11 illustrates an example of a method for ownership determination.

FIG. 12 illustrates an example of a method for determining permissions.

FIG. 13 illustrates an example of a method for detecting identified information.

DESCRIPTION

Unless specifically stated otherwise, as apparent from the following discussions, it is appreciated that throughout the specification discussions utilizing terms such as “processing”, “calculating”, “computing”, “determining”, “generating”, “setting”, “configuring”, “selecting”, “defining”, “applying”, “obtaining”, “monitoring”, “providing”, “identifying”, “segmenting”, “classifying”, “analyzing”, “associating”, “extracting”, “storing”, “receiving”, “transmitting”, or the like, include action and/or processes of a computer that manipulate and/or transform data into other data, said data represented as physical quantities, for example such as electronic quantities, and/or said data representing the physical objects. The terms “computer”, “processor”, “controller”, “processing unit”, “computing device”, and “processing module” should be expansively construed to cover any kind of electronic device, component or unit with data processing capabilities, including, by way of non-limiting example, a personal computer, a wearable computer, a tablet, a smartphone, a server, a computing system, a cloud computing platform, a communication device, a processor (for example, digital signal processor (DSP), an image signal processor (ISR), a microcontroller, a field programmable gate array (FPGA), an application specific integrated circuit (ASIC), a central processing unit (CPA), a graphics processing unit (GPU), a visual processing unit (VPU), and so on), possibly with embedded memory, a single core

5

processor, a multi core processor, a core within a processor, any other electronic computing device, or any combination of the above.

The operations in accordance with the teachings herein may be performed by a computer specially constructed or programmed to perform the described functions.

As used herein, the phrase “for example,” “such as,” “for instance” and variants thereof describe non-limiting embodiments of the presently disclosed subject matter. Reference in the specification to “one case,” “some cases,” “other cases” or variants thereof means that a particular feature, structure or characteristic described in connection with the embodiment(s) may be included in at least one embodiment of the presently disclosed subject matter. Thus the appearance of the phrase “one case,” “some cases,” “other cases” or variants thereof does not necessarily refer to the same embodiment(s). As used herein, the term “and/or” includes any and all combinations of one or more of the associated listed items.

It is appreciated that certain features of the presently disclosed subject matter, which are, for clarity, described in the context of separate embodiments, may also be provided in combination in a single embodiment. Conversely, various features of the presently disclosed subject matter, which are, for brevity, described in the context of a single embodiment, may also be provided separately or in any suitable sub-combination.

In embodiments of the presently disclosed subject matter, one or more stages illustrated in the figures may be executed in a different order and/or one or more groups of stages may be executed simultaneously and vice versa. The figures illustrate a general schematic of the system architecture in accordance with embodiments of the presently disclosed subject matter. Each module in the figures can be made up of any combination of software, hardware and/or firmware that performs the functions as defined and explained herein. The modules in the figures may be centralized in one location or dispersed over more than one location.

It should be noted that some examples of the presently disclosed subject matter are not limited in application to the details of construction and the arrangement of the components set forth in the following description or illustrated in the drawings. The invention can be capable of other embodiments or of being practiced or carried out in various ways. Also, it is to be understood that the phraseology and terminology employed herein is for the purpose of description and should not be regarded as limiting.

In this document, an element of a drawing that is not described within the scope of the drawing and is labeled with a numeral that has been described in a previous drawing may have the same use and description as in the previous drawings.

The drawings in this document may not be to any scale. Different figures may use different scales and different scales can be used even within the same drawing, for example different scales for different views of the same object or different scales for the two adjacent objects.

FIG. 1 is an illustration of an exemplary system 100 for providing information based on medical data. In some examples, system 100 may include one or more medical organizations 110 (in this example, medical organizations 110A, 110B and 110C). Some possible examples of such medical organizations 110 may include hospitals, medical clinics, medical labs, pharmacies, medical care providers 630 (described below), insurers 640 (described below), regulators 650 (described below), and so forth. Each one of the one or more medical organizations 110 may hold private

6

medical data. In this example, medical organization 110A holds private medical data 112. Access to all or portions of private medical data 112 may be restricted, for example due to regulatory and privacy requirements, due to medical organization 110 procedures, and so forth. Some examples of such medical data 112 may include medical records 702 (described below), scheduling records 704 (described below), financial records 706 (described below), insurance records 708 (described below), research records 710 (described below), and so forth. In some examples, system 100 may include public data 120. Access to public data may be publically available to everyone. In some examples, system 100 may include one or more teams 140 (in this example, teams 140A, 140B and 140C). Some possible examples of such teams 140 may include research teams, research organizations, individual researchers, researchers 660 (described below), insurers 640 (described below), regulators 650 (described below), and so forth. In some example, each one of the one or more teams 140 may hold proprietary medical data. In this example, team 140A holds proprietary medical data 142. In some example, each one of the one or more teams 140 may use computerized data analysis devices. In this example, team 140A uses computerized data analysis device 144. Some possible implementations of computerized data analysis device 144 may include computing device 200 (described below), cloud platform 400 (described below), computational node 500 (described below), and so forth. In some example, each one of the one or more teams 140 may include one or more users. In this example, team 140A includes users 146, 147 and 148. Some possible examples of such users may include researchers 660 (described below), human data analysts, automated data analyst processes, and so forth. In some examples, data may be exchanged among elements of system 100, for example through communication network 130. Examples of communication network 130 may include the Internet, phone networks, cellular networks, satellite communication networks, private communication networks, virtual private networks (VPN), and so forth. Computerized devices (such as computing device 200, cloud platform 400, computational node 500, computerized data analysis device 144, storage devices, local storage, remote storage, network attached storage, etc.) may connect to communication network 130 directly, through local router, through wireless communication, through wired communication, and so forth.

In some examples, at least a portion of at least one of private medical data 112, public data 120 and proprietary medical data 142 may be stored in memory (such as memory 700, memory units 210, memory modules 410, etc.), in storage device (such as local storage, remote storage, network attached storage, etc.), and so forth. In some examples, at least a portion of at least one of private medical data 112, public data 120 and proprietary medical data 142 may be managed and/or controlled and/or maintained and/or collected and/or analyzed using local computing devices (such as computing device 200), local computerized servers, remote computerized servers, private and/or public cloud platforms (such as cloud platform 400), computational node (such as computational node 500), and so forth.

In some embodiments, a privacy firewall may be used to control access to data and enforce privacy rules. For example, a privacy firewall may be implemented using a computing device (such as computing device 200), may be implemented using a cloud platform (such as cloud platform 400), may be implemented as a software (for example in an operation system, as a software configured to be installed on a computing device, etc.), and so forth. In one example, a

privacy firewall may be positioned on the connection between medical organization **110A** and external network **130**, for example to control all access to data in medical organization **110A** from external entities and enforce privacy rules on access to data in medical organization **110A** through network **130**. In another example, a privacy firewall may be positioned on the connection between team **140A** and external network **130**, for example to control all access to external data from team **140A** and enforce privacy rules on access of team **140A** to data through network **130**. In yet another example, a privacy firewall may be positioned within medical organization **110A** to control access to private medical data **112**, for example to control all access to private medical data **112**, whether the access is coming from within medical organization **110A** or from external sources and enforce privacy rules on access to private medical data **112**. In an additional example, a privacy firewall may be installed on computerized data analysis device **144**, for example to control all access to data from computerized data analysis device **144** and enforce privacy rules on access of computerized data analysis device **144** to data.

FIG. **2A** is a block diagram illustrating a possible implementation of computing device **200**. In this example, computing device **200** may comprise: one or more memory units **210**, one or more processing units **220**, and one or more communication modules **230**. In some implementations, computing device **200** may comprise additional components, while some components listed above may be excluded.

FIG. **2B** is a block diagram illustrating a possible implementation of computing device **200**. In this example, computing device **200** may comprise: one or more memory units **210**, one or more processing units **220**, one or more communication modules **230**, one or more power sources **240**, one or more audio sensors **250**, one or more image sensors **260**, one or more light sources **265**, one or more motion sensors **270**, and one or more positioning sensors **275**. In some implementations, computing device **200** may comprise additional components, while some components listed above may be excluded. For example, in some implementations computing device **200** may also comprise at least one of the following: one or more barometers; one or more user input devices; one or more output devices; and so forth. In another example, in some implementations at least one of the following may be excluded from computing device **200**: memory units **210**, communication modules **230**, power sources **240**, audio sensors **250**, image sensors **260**, light sources **265**, motion sensors **270**, and positioning sensors **275**.

In some embodiments, one or more power sources **240** may be configured to: power computing device **200**, power cloud platform **400**, and/or power computational node **500**. Possible implementation examples of power sources **240** may include: one or more electric batteries; one or more capacitors; one or more connections to external power sources; one or more power convertors; any combination of the above; and so forth.

In some embodiments, the one or more processing units **220** may be configured to execute software programs. For example, processing units **220** may be configured to execute software programs stored on the memory units **210**. In some cases, the executed software programs may store information in memory units **210**. In some cases, the executed software programs may retrieve information from the memory units **210**. Possible implementation examples of the processing units **220** may include: one or more single core processors, one or more multicore processors; one or more

controllers; one or more application processors; one or more system on a chip processors; one or more central processing units; one or more graphical processing units; one or more neural processing units; any combination of the above; and so forth.

In some embodiments, the one or more communication modules **230** may be configured to receive and transmit information. For example, control signals may be transmitted and/or received through communication modules **230**. In another example, information received through communication modules **230** may be stored in memory units **210**. In an additional example, information retrieved from memory units **210** may be transmitted using communication modules **230**. In another example, input data may be transmitted and/or received using communication modules **230**. Examples of such input data may include: input data inputted by a user using user input devices; information captured using one or more sensors; and so forth. Examples of such sensors may include: audio sensors **250**; image sensors **260**; motion sensors **270**; positioning sensors **275**; chemical sensors; temperature sensors; barometers; and so forth.

In some embodiments, the one or more audio sensors **250** may be configured to capture audio by converting sounds to digital information. Some examples of audio sensors **250** may include: microphones, unidirectional microphones, bidirectional microphones, cardioid microphones, omnidirectional microphones, onboard microphones, wired microphones, wireless microphones, any combination of the above, and so forth. In some examples, the captured audio may be stored in memory units **210**. In some additional examples, the captured audio may be transmitted using communication modules **230**, for example to other computerized devices, such as cloud platform **400**, computational node **500**, and so forth. In some examples, processing units **220** may control the above processes. For example, processing units **220** may control at least one of: capturing of the audio; storing the captured audio; transmitting of the captured audio; and so forth. In some cases, the captured audio may be processed by processing units **220**. For example, the captured audio may be compressed by processing units **220**; possibly followed: by storing the compressed captured audio in memory units **210**; by transmitted the compressed captured audio using communication modules **230**; and so forth. In another example, the captured audio may be processed using speech recognition algorithms. In another example, the captured audio may be processed using speaker recognition algorithms.

In some embodiments, an image sensor **260** may include a device configured to capture images, a sequence of images, videos, and so forth. This includes sensors that convert optical input into images, where optical input can be visible light (like in a camera), radio waves, microwaves, terahertz waves, ultraviolet light, infrared light, x-rays, gamma rays, and/or any other light spectrum. This also includes both 2D and 3D sensors. Examples of image sensor technologies may include: CCD, CMOS, NMOS, and so forth. 3D sensors may be implemented using different technologies, including: stereo camera, active stereo camera, time of flight camera, structured light camera, radar, range image camera, and so forth. In some examples, the one or more image sensors **260** may be configured to capture visual information by converting light to: images; sequence of images; videos; 3D images; sequence of 3D images; 3D videos; and so forth. In some examples, the captured visual information may be stored in memory units **210**. In some additional examples, the captured visual information may be transmitted using communication modules **230**, for example to other computerized

devices, such as cloud platform **400**, computational node **500**, and so forth. In some examples, processing units **220** may control the above processes. For example, processing units **220** may control at least one of: capturing of the visual information; storing the captured visual information; transmitting of the captured visual information; and so forth. In some cases, the captured visual information may be processed by processing units **220**. For example, the captured visual information may be compressed by processing units **220**; possibly followed: by storing the compressed captured visual information in memory units **210**; by transmitted the compressed captured visual information using communication modules **230**; and so forth. In another example, the captured visual information may be processed in order to: detect objects, detect events, detect action, detect face, detect people, recognize person, and so forth.

In some embodiments, the one or more light sources **265** may be configured to emit light, for example in order to enable better image capturing by image sensors **260**. In some examples, the emission of light may be coordinated with the capturing operation of image sensors **260**. In some examples, the emission of light may be continuous. In some examples, the emission of light may be performed at selected times. The emitted light may be visible light, infrared light, x-rays, gamma rays, and/or in any other light spectrum. In some examples, image sensors **260** may capture light emitted by light sources **265**, for example in order to capture 3D images and/or 3D videos using active stereo method.

In some embodiments, the one or more motion sensors **270** may be configured to perform at least one of the following: detect motion of objects in the environment of computing device **200**; measure the velocity of objects in the environment of computing device **200**; measure the acceleration of objects in the environment of computing device **200**; detect motion of computing device **200**; measure the velocity of computing device **200**; measure the acceleration of computing device **200**; and so forth. In some implementations, the one or more motion sensors **270** may comprise one or more accelerometers configured to detect changes in proper acceleration and/or to measure proper acceleration of computing device **200**. In some implementations, the one or more motion sensors **270** may comprise one or more gyroscopes configured to detect changes in the orientation of computing device **200** and/or to measure information related to the orientation of computing device **200**. In some implementations, motion sensors **270** may be implemented using image sensors **260**, for example by analyzing images captured by image sensors **260** to perform at least one of the following tasks: track objects in the environment of computing device **200**; detect moving objects in the environment of computing device **200**; measure the velocity of objects in the environment of computing device **200**; measure the acceleration of objects in the environment of computing device **200**; measure the velocity of computing device **200**, for example by calculating the egomotion of image sensors **260**; measure the acceleration of computing device **200**, for example by calculating the egomotion of image sensors **260**; and so forth. In some implementations, motion sensors **270** may be implemented using image sensors **260** and light sources **265**, for example by implementing a LIDAR using image sensors **260** and light sources **265**. In some implementations, motion sensors **270** may be implemented using one or more RADARs. In some examples, information captured using motion sensors **270**: may be stored in memory units **210**, may be processed by processing units

220, may be transmitted and/or received using communication modules **230**, and so forth.

In some embodiments, the one or more positioning sensors **275** may be configured to obtain positioning information of computing device **200**, to detect changes in the position of computing device **200**, and/or to measure the position of computing device **200**. In some examples, positioning sensors **275** may be implemented using one of the following technologies: Global Positioning System (GPS), GLObal NAVigation Satellite System (GLONASS), Galileo global navigation system, BeiDou navigation system, other Global Navigation Satellite Systems (GNSS), Indian Regional Navigation Satellite System (IRNSS), Local Positioning Systems (LPS), Real-Time Location Systems (RTLS), Indoor Positioning System (IPS), Wi-Fi based positioning systems, cellular triangulation, and so forth. In some examples, information captured using positioning sensors **275** may be stored in memory units **210**, may be processed by processing units **220**, may be transmitted and/or received using communication modules **230**, and so forth.

In some embodiments, the one or more chemical sensors may be configured to perform at least one of the following: measure chemical properties in the environment of computing device **200**; measure changes in the chemical properties in the environment of computing device **200**; detect the present of chemicals in the environment of computing device **200**; measure the concentration of chemicals in the environment of computing device **200**. Examples of such chemical properties may include: pH level, toxicity, temperature, and so forth. Examples of such chemicals may include: electrolytes, particular enzymes, particular hormones, particular proteins, smoke, carbon dioxide, carbon monoxide, oxygen, ozone, hydrogen, hydrogen sulfide, and so forth. In some examples, information captured using chemical sensors may be stored in memory units **210**, may be processed by processing units **220**, may be transmitted and/or received using communication modules **230**, and so forth.

In some embodiments, the one or more temperature sensors may be configured to detect changes in the temperature of the environment of computing device **200** and/or to measure the temperature of the environment of computing device **200**. In some examples, information captured using temperature sensors may be stored in memory units **210**, may be processed by processing units **220**, may be transmitted and/or received using communication modules **230**, and so forth.

In some embodiments, the one or more barometers may be configured to detect changes in the atmospheric pressure in the environment of computing device **200** and/or to measure the atmospheric pressure in the environment of computing device **200**. In some examples, information captured using the barometers may be stored in memory units **210**, may be processed by processing units **220**, may be transmitted and/or received using communication modules **230**, and so forth.

In some embodiments, the one or more user input devices may be configured to allow one or more users to input information. In some examples, user input devices may comprise at least one of the following: a keyboard, a mouse, a touch pad, a touch screen, a joystick, a microphone, an image sensor, and so forth. In some examples, the user input may be in the form of at least one of: text, sounds, speech, hand gestures, body gestures, tactile information, and so forth. In some examples, the user input may be stored in memory units **210**, may be processed by processing units

11

220, may be transmitted and/or received using communication modules 230, and so forth.

In some embodiments, the one or more user output devices may be configured to provide output information to one or more users. In some examples, such output information may comprise of at least one of: notifications, feedbacks, reports, and so forth. In some examples, user output devices may comprise at least one of: one or more audio output devices; one or more textual output devices; one or more visual output devices; one or more tactile output devices; and so forth. In some examples, the one or more audio output devices may be configured to output audio to a user, for example through: a headset, a set of speakers, and so forth. In some examples, the one or more visual output devices may be configured to output visual information to a user, for example through: a display screen, an augmented reality display system, a printer, a LED indicator, and so forth. In some examples, the one or more tactile output devices may be configured to output tactile feedbacks to a user, for example through vibrations, through motions, by applying forces, and so forth. In some examples, the output may be provided: in real time, offline, automatically, upon request, and so forth. In some examples, the output information may be read from memory units 210, may be provided by a software executed by processing units 220, may be transmitted and/or received using communication modules 230, and so forth.

FIG. 3 is a block diagram illustrating a possible implementation of a communicating system. In this example, computing devices 200a, 200b and 200c may communicate with cloud platform 400 and/or with each other through communication network 130. Possible implementations of computing devices 200a, 200b and 200c may include computing device 200 as described in FIGS. 2A and/or 2B. Some possible implementations of cloud platform 400 are described in FIGS. 4A, 4B and 5.

FIG. 3 illustrates a possible implementation of a communication system. In some embodiments, other communication systems that enable communication among computing devices and/or between a computing device (such as computing device 200) and a cloud platform (such as cloud platform 400) may be used.

FIG. 4A is a block diagram illustrating a possible implementation of cloud platform 400. In this example, cloud platform 400 may comprise computational node 500a, computational node 500b, computational node 500c and computational node 500d. In some examples, a possible implementation of computational nodes 500a, 500b, 500c and 500d may comprise computing device 200. In some examples, a possible implementation of computational nodes 500a, 500b, 500c and 500d may comprise computational node 500 as described in FIG. 5.

FIG. 4B is a block diagram illustrating a possible implementation of cloud platform 400. In this example, cloud platform 400 may comprise: one or more computational nodes 500, one or more shared memory modules 410, one or more power sources 240, one or more node registration modules 420, one or more load balancing modules 430, one or more internal communication modules 440, and one or more external communication modules 450. In some implementations, cloud platform 400 may comprise additional components, while some components listed above may be excluded. For example, in some implementations cloud platform 400 may also comprise at least one of the following: one or more user input devices; one or more output devices; and so forth. In another example, in some implementations at least one of the following may be excluded

12

from cloud platform 400: shared memory modules 410, power sources 240, node registration modules 420, load balancing modules 430, internal communication modules 440, and external communication modules 450.

FIG. 5 is a block diagram illustrating a possible implementation of computational node 500. In this example, computational node 500 may comprise: one or more memory units 210, one or more processing units 220, one or more shared memory access modules 510, one or more power sources 240, one or more internal communication modules 440, and one or more external communication modules 450. In some implementations, computational node 500 may comprise additional components, while some components listed above may be excluded. For example, in some implementations computational node 500 may also comprise at least one of the following: one or more user input devices; one or more output devices; and so forth. In another example, in some implementations at least one of the following may be excluded from computational node 500: memory units 210, shared memory access modules 510, power sources 240, internal communication modules 440, and external communication modules 450.

In some embodiments, internal communication modules 440 and external communication modules 450 may be implemented as a combined communication module, such as communication modules 230. In some embodiments, one possible implementation of cloud platform 400 may comprise computing device 200. In some embodiments, one possible implementation of computational node 500 may comprise computing device 200. In some embodiments, one possible implementation of shared memory access modules 510 may comprise using internal communication modules 440 to send information to shared memory modules 410 and/or receive information from shared memory modules 410. In some embodiments, node registration modules 420 and load balancing modules 430 may be implemented as a combined module.

In some embodiments, the one or more shared memory modules 410 may be accessed by more than one computational node. Therefore, shared memory modules 410 may allow information sharing among two or more computational nodes 500. In some embodiments, the one or more shared memory access modules 510 may be configured to enable access of computational nodes 500 and/or the one or more processing units 220 of computational nodes 500 to shared memory modules 410. In some examples, computational nodes 500 and/or the one or more processing units 220 of computational nodes 500, may access shared memory modules 410, for example using shared memory access modules 510, in order to perform at least one of: executing software programs stored on shared memory modules 410, store information in shared memory modules 410, retrieve information from the shared memory modules 410.

In some embodiments, the one or more node registration modules 420 may be configured to track the availability of the computational nodes 500. In some examples, node registration modules 420 may be implemented as: a software program, such as a software program executed by one or more of the computational nodes 500; a hardware solution; a combined software and hardware solution; and so forth. In some implementations, node registration modules 420 may communicate with computational nodes 500, for example using internal communication modules 440. In some examples, computational nodes 500 may notify node registration modules 420 of their status, for example by sending messages: at computational node 500 startup; at computational node 500 shutdown; at constant intervals; at selected

13

times; in response to queries received from node registration modules **420**; and so forth. In some examples, node registration modules **420** may query about computational nodes **500** status, for example by sending messages: at node registration module **420** startup; at constant intervals; at selected times; and so forth.

In some embodiments, the one or more load balancing modules **430** may be configured to divide the work load among computational nodes **500**. In some examples, load balancing modules **430** may be implemented as: a software program, such as a software program executed by one or more of the computational nodes **500**; a hardware solution; a combined software and hardware solution; and so forth. In some implementations, load balancing modules **430** may interact with node registration modules **420** in order to obtain information regarding the availability of the computational nodes **500**. In some implementations, load balancing modules **430** may communicate with computational nodes **500**, for example using internal communication modules **440**. In some examples, computational nodes **500** may notify load balancing modules **430** of their status, for example by sending messages: at computational node **500** startup; at computational node **500** shutdown; at constant intervals; at selected times; in response to queries received from load balancing modules **430**; and so forth. In some examples, load balancing modules **430** may query about computational nodes **500** status, for example by sending messages: at load balancing module **430** startup; at constant intervals; at selected times; and so forth.

In some embodiments, the one or more internal communication modules **440** may be configured to receive information from one or more components of cloud platform **400**, and/or to transmit information to one or more components of cloud platform **400**. For example, control signals and/or synchronization signals may be sent and/or received through internal communication modules **440**. In another example, input information for computer programs, output information of computer programs, and/or intermediate information of computer programs, may be sent and/or received through internal communication modules **440**. In another example, information received through internal communication modules **440** may be stored in memory units **210**, in shared memory units **410**, and so forth. In an additional example, information retrieved from memory units **210** and/or shared memory units **410** may be transmitted using internal communication modules **440**. In another example, input data may be transmitted and/or received using internal communication modules **440**. Examples of such input data may include input data inputted by a user using user input devices.

In some embodiments, the one or more external communication modules **450** may be configured to receive and/or to transmit information. For example, control signals may be sent and/or received through external communication modules **450**. In another example, information received through external communication modules **450** may be stored in memory units **210**, in shared memory units **410**, and so forth. In an additional example, information retrieved from memory units **210** and/or shared memory units **410** may be transmitted using external communication modules **450**. In another example, input data may be transmitted and/or received using external communication modules **450**. Examples of such input data may include: input data inputted by a user using user input devices; information captured from the environment of computing device **200** using one or more sensors; and so forth. Examples of such sensors may include: audio sensors **250**; image sensors **260**; motion

14

sensors **270**; positioning sensors **275**; chemical sensors; temperature sensors; barometers; and so forth.

FIG. **6** is a block diagrams illustrating a possible ecosystem **600**. In this example, the ecosystem may comprise one or more patients **610**, one or more relatives **620**, one or more medical care providers **630**, one or more insurers **640**, one or more regulators **650**, one or more researchers **660**, and one or more facilitators **670**. In some embodiments, other ecosystems may exist. In some examples, ecosystem **600** may comprise one or more additional entities, while some of the entities listed above may be excluded from ecosystem **600**. For example, patients **610** and/or relatives **620** and/or medical care providers **630** and/or insurers **640** and/or regulators **650** and/or researchers **660** and/or facilitators **670** may be excluded from ecosystem **600**. For example, ecosystem **600** may further include financial institutes (such as banks, credit companies, etc.), legal firms, non-medical service providers, research institutes, and so forth.

In some embodiments, entities of ecosystem **600** (such as patients **610**, relatives **620**, medical care providers **630**, insurers **640**, regulators **650**, researcher **660**, facilitators **670**, etc.) may use computerized devices (such as computing device **200**, computational node **500**, cloud platform **400**, etc.) to perform part and/or all of their functions and/or duties. For example, the entities may use computerized devices to store and/or access and/or process data (some examples of such data may include medical records **702**, scheduling records **704**, financial records **706**, insurance records **708**, research records **710**, indexes **712**, identifiers **714**, and/or permissions **716** described below), to communicate (for example over communication network **130**), and so forth.

In some embodiments, patients **610** may comprise one or more individuals that received and/or are about to receive medical care.

In some embodiments, relatives **620** may comprise one or more individuals that have some bearing on the medical care of at least one patient **610**. For example, relatives **620** may comprise one or more of a family member of patient **610**, a friend of patient **610**, a legal guardian of patient **610**, a next of kin of patient **610**, a non-medical care giver of patient **610**, and so forth.

In some embodiments, medical care providers **630** may comprise one or more individual and/or one or more institutes that provides (in the past and/or present and/or future) medical care to patients **610**. For example, medical care providers **630** may comprise one or more medical care professionals (such as medical doctors, nurses, therapists, staff of medical care institutes, etc.), one or more medical care institutes (such as hospitals, clinics, labs, etc.), and so forth.

In some embodiments, insurers **640** may comprise one or more individuals and/or one or more institutes that cover medical expenses (such as medical expenses of at least some of patients **610** and/or medical care providers **630**) and/or insures medical care providers **630** for malpractice costs. In some examples, insurers may include insurance firms and/or government agencies.

In some embodiments, regulators **650** may comprise official entities appointed to track and/or regulate the medical care provided to patents **610** and/or the medical care provided by medical care providers **630** and/or the medical care covered by insurers **640**. For example, regulators **650** may comprise government agencies (such as the FDA, NIH, EMA, CFDA, PMDA, etc.), professional associations (such as the WMA, AMA, EMA, CMA, JMA, etc.), court appointed oversight, and so forth.

15

In some embodiments, researcher **660** may comprise research personals, research facilities, research institutes, research teams (such as teams **140A**, **140B** and **140C**), and so forth. For example, researchers **660** may comprise a university, a drug development company, a research profes-

sor, and so forth. In some embodiments, facilitators **670** may comprise individuals and/or entities that facilitate the communication among entities of ecosystem **600**.

FIG. 7A illustrates an exemplary embodiment of memory **700** storing a plurality of modules. In some examples, memory **700** may be separate from and/or integrated with memory units **210**, separate from and/or integrated with memory units **410**, and so forth. In some examples, memory **700** may be included in a single device, for example in computing device **200**, in cloud platform **400**, in computational node **500**, and so forth. In some examples, memory **700** may be distributed across several devices. Memory **700** may store more or fewer modules than those shown in FIG. 7A. In this example, memory **700** may comprise: medical records **702**, scheduling records **704**, financial records **706**, insurance records **708**, research records **710**, indexes **712**, identifiers **714**, and permissions **716**.

In some embodiments, at least part of medical records **702** scheduling records **704**, financial records **706**, insurance records **708**, research records **710**, indexes **712**, identifiers **714**, and/or permissions **716** may be stored in a public database, in a public ledger, in a blockchain, in a computerized devices (such as computing device **200**, cloud platform **400**, computational node **500**, etc.), in a storage devices (such as remote storage, network attached storage, etc.), and so forth. In some examples, medical records **702**, scheduling records **704**, financial records **706**, insurance records **708**, research records **710**, indexes **712**, identifiers **714**, and/or permissions **716** may be stored in single database and/or blockchain and/or site and/or device, while in other examples medical records **702** may be distributed among a number of databases and/or blockchains and/or sites and/or devices. In some examples, medical records of a single entity (such as patient **610**, relative **620**, medical care provider **630**, insurer **640**, regulator **650**, researcher **660**, facilitator **670**, etc.) may be stored in single database and/or blockchain and/or site and/or device, while in other examples the medical records of the entity may be distributed among a number of databases and/or blockchains and/or sites and/or devices.

In some embodiments, medical records **702** may comprise medical records of one or more patients **610**, medical records created and/or used by one or more medical care providers **630**, medical records associated with one or more patients and/or medical care providers insured by one or more insurers **640**, medical records surveyed by one or more regulators **650**, medical records studied by one or more researchers **660**, and so forth. In some examples, medical records **702** may comprise medical information, such as information regarding medical conditions, medical care, medical treatment, EHR, genome data, and so forth.

In some embodiments, scheduling records **704** may comprise scheduling related information associated with patients **610** and/or relatives **620** and/or medical care providers **630** and/or insurers **640** and/or regulators **650** and/or researchers **660** and/or facilitators **670**. The scheduling related information may relate to past and/or present and/or future events. For example, scheduling records **704** may comprise time and date information for an appointment, for a lab test, for a medical exam, for a medical checkup, for a reminder related to medical care, and so forth.

16

In some embodiments, financial records **706** may comprise financial information associated with patients **610** and/or relatives **620** and/or medical care providers **630** and/or insurers **640** and/or regulators **650** and/or researchers **660** and/or facilitators **670**. The financial information may relate to past, present, and/or future budget, costs, bills, coverage obligations, and/or payments associated with medical care.

In some embodiments, insurance records **708** may comprise insurance information associated with patients **610** and/or relatives **620** and/or medical care providers **630** and/or insurers **640** and/or regulators **650** and/or researchers **660** and/or facilitators **670**. The insurance information may include past, present and/or future coverage information, insurance claims, insurance payments, and so forth, associated with medical care.

In some embodiments, research records **710** may comprise research records associated with patients **610** and/or relatives **620** and/or medical care providers **630** and/or insurers **640** and/or regulators **650** and/or researchers **660** and/or facilitators **670**. For example, research records **710** may comprise research records compiled and/or studied by a researcher **660**. For example, research records **710** may comprise research records pertaining to one or more medical researches.

In some embodiments, indexes **712** may comprise one or more partial and/or complete indexes. In some examples, an index may link an identifier of a record (such as medical record **702** scheduling record **704**, financial record **706**, insurance record **708**, research record **710**, index **712**, identifiers **714**, permission **716**, etc.) to entities (such as patients **610**, relatives **620**, medical care providers **630**, insurers **640**, regulators **650**, researchers **660**, facilitators **670**, and so forth). For example, an index may link an identifier of a record to the entity created the record, to entities that accessed and/or edited the record, to entities that has permission to access and/or edit the record, and so forth.

In some examples, an index may link an identifier of an entity (such as patient **610**, relative **620**, medical care provider **630**, insurer **640**, regulator **650**, researcher **660**, facilitator **670**, etc.) to records (such as medical records **702** scheduling records **704**, financial records **706**, insurance records **708**, research records **710**, indexes **712**, identifiers **714**, permissions **716**, etc.) associated with the entity, to records that the entity has permissions to access and/or edit, to records accessed and/or edited by the entity, and so forth.

In some examples, an index may link an identifier of an entity (such as patient **610**, relative **620**, medical care provider **630**, insurer **640**, regulator **650**, researcher **660**, facilitator **670**, etc.) to computerized devices (such as computing device **200**, computational node **500**, cloud platform **400**, etc.) and/or to storage devices (such as remote storage, network attached storage, etc.) and/or to blockchains and/or to databases containing information and/or at least part of the records (such as medical records **702** scheduling records **704**, financial records **706**, insurance records **708**, research records **710**, indexes **712**, identifiers **714**, permissions **716**, etc.) associated with the entity.

In some examples, an index may link an identifier of an entity (such as patient **610**, relative **620**, medical care provider **630**, insurer **640**, regulator **650**, researcher **660**, facilitator **670**, etc.) to other entities (such as patient **610**, relative **620**, medical care provider **630**, insurer **640**, regulator **650**, researcher **660**, facilitator **670**, and so forth). For example, an index may link an identifier of a patient **610** to relatives **620** related to the patient, medical care providers **630** that created and/or hold at least part of the records

associated with the patient, to medical care providers **630** that hold permissions to access and/or edit at least parts of the records associated with the patient, to medical care providers **630** that accessed and/or edited at least parts of the records associated with the patient, to one or more insurers **640** associated with the patient, to regulators **650** dealing with medical information related to the patient, to researchers **660** studying medical information related to the patient, and so forth. For example, an index may link an identifier of a relative **620** to a patient **610** related to the relative and/or to entities associated with that patient. For example, an index may link an identifier of a medical care provider **630** to patients **610** and/or relatives of patient **620** that the medical care provider treat and/or has permissions to access and/or edit at least part of their medical records, to other medical care providers **630** that work in conjunction with the medical care provider, to insurer **640** of the medical care provider and/or patients of the medical care provider and/or employees of the medical care provider and/or suppliers of the medical care provider, to regulators **650** supervising the medical care provider, to researchers **660** working with and/or for the medical care provider, and so forth. For example, an index may link an identifier of an insurer **640** to entities insured by the insurer. For example, an index may link an identifier of a regulator **650** to entities supervised by the regulator. For example, an index may link an identifier of a researcher **660** to entities studied by the researcher, to entities working in conjunction with the researcher, and so forth. For example, an index may link an identifier of a facilitator **670** to entities recognized by and/or associated with the facilitator.

In some embodiments, identifiers **714** may comprise identifiers of entities (such as patients **610**, relatives **620**, medical care providers **630**, insurers **640**, regulators **650**, researchers **660**, facilitators **670**, etc.) and/or records (such as medical records **702** scheduling records **704**, financial records **706**, insurance records **708**, research records **710**, indexes **712**, permissions **716**, and so forth). In some examples, identifier of an entity and/or record may be unique, while in other examples more than one identifier may identify the same entity and/or record.

In some embodiments, permissions **716** may specify which entities (such as patients **610**, relatives **620**, medical care providers **630**, insurers **640**, regulators **650**, researchers **660**, facilitators **670**, etc.) may create and/or edit and/or access which records (such as medical records **702** scheduling records **704**, financial records **706**, insurance records **708**, research records **710**, indexes **712**, identifiers **714**, permissions **716**, and so forth). For example, permissions **716** may comprise a group or entities allowed to create and/or edit and/or access selected records, a group or entities prohibited from creating and/or editing and/or accessing selected records, and so forth. For example, the selected records above may be specified as a group of records, as a rule defining a group of records, as the records associated with selected entities, and so forth. In some examples, permissions **716** may further specify which entities are allowed to grant which permission to which other entities regarding which records.

In some embodiments, medical care providers **630** may create and/or edit records of a patient **610** (such as medical records **702** scheduling records **704**, financial records **706**, insurance records **708**, research records **710**, indexes **712**, identifiers **714**, permissions **716**, and so forth). These records may be indexed in indexes **712**. These records may be accessed and/or edited by the patient, by some relatives **620** of the patient, by other medical care providers **630**

treating the patient, by insurers **640** of the patient and/or the medical care provider, and so forth.

In some embodiments, an insurer **640** may access and/or edit and/or create records (such as medical records **702** scheduling records **704**, financial records **706**, insurance records **708**, research records **710**, indexes **712**, identifiers **714**, permissions **716**, etc.) of entities (such as patients **610**, relatives **620**, medical care providers **630**, other insurers **640**, regulators **650**, researchers **660**, facilitators **670**, etc.) insured by the insurer.

In some embodiments, a regulator **650** may access and/or edit and/or create records (such as medical records **702** scheduling records **704**, financial records **706**, insurance records **708**, research records **710**, indexes **712**, identifiers **714**, permissions **716**, etc.) of entities (such as patients **610**, relatives **620**, medical care providers **630**, other insurers **640**, regulators **650**, researchers **660**, facilitators **670**, etc.) supervised by the regulator.

In some embodiments, a researcher **660** may access and/or edit and/or create records (such as medical records **702** scheduling records **704**, financial records **706**, insurance records **708**, research records **710**, indexes **712**, identifiers **714**, permissions **716**, etc.) of entities (such as patients **610**, relatives **620**, medical care providers **630**, other insurers **640**, regulators **650**, researchers **660**, facilitators **670**, etc.) studied by the researcher.

In some embodiments, a facilitator **670** may access and/or edit and/or create records (such as medical records **702** scheduling records **704**, financial records **706**, insurance records **708**, research records **710**, indexes **712**, identifiers **714**, permissions **716**, etc.) of entities (such as patients **610**, relatives **620**, medical care providers **630**, other insurers **640**, regulators **650**, researchers **660**, facilitators **670**, and so forth). For example, a facilitator **670** may create an identifier **714**, may verify an identity **714**, and so forth. For example, a facilitator **670** may provide permission to relatives **620** of a patient **610** to access the patient's record after the death of the patient by editing permissions **716**. For example, a facilitator **670** may recognize an entity as a licensed medical professional, as a licensed insurer, as a legitimate researcher, as a legal regulator, and so forth.

In some embodiments, access to a record and/or creation of a record and/or edition to a record may be recorded, for example in a log, in indexes **712**, in the accessed and/or created and/or edited record, and so forth.

FIG. 7B illustrates an exemplary embodiment of a data element **730**. In some examples, data element **730** may be stored in a memory unit (such as memory **700**), in a database, in a data structure, in a table, and so forth. In some examples, data element **730** may comprise one or more data fields. For example, in the example of FIG. 7B data element **730** may comprise patient name **732**, patient address **734**, patient age **736**, physician name **738** and medication data **740**. In some examples, data element **730** may include portion **742** that includes identifiable information of a patient (in this example, portion **742** may include data fields patient name **732** and patient address **734**), and portion **744** that does not include identifiable information of a patient (in this example, portion **744** may include data fields patient age **736**, physician name **738** and medication data **740**). In some examples, data element **730** may include additional portions and/or data fields that are not included in portion **742** and portion **744**.

FIG. 7C illustrates an exemplary embodiment of a data element **750**. In some examples, data element **750** may be stored in a memory unit (such as memory **700**), in a database, in a data structure, in a table, and so forth. In some

examples, data element **750** may comprise a table including one or more columns. For example, in the example of FIG. 7C data element **750** may comprise patient name column **752**, patient phone number column **754**, physician name **756** and appointment time **758**. In some examples, data element **750** may include portions that includes identifiable information of a patient and portions that does not include identifiable information of a patient. The division of data element **750** to portions that includes identifiable information of a patient and portions that does not include identifiable information of a patient may be based on the type of the column (for example, patient name column **752** and patient phone number column **754** may be identified as including identifiable information of a patient based on the type of the column), may be based on a distribution of values in the column (for example, in clinics that only have one or few appointments at the same time, appointment time column **758** may be identified as including identifiable information of a patient based on the distribution of appointment times in the column, while in clinics that have many appointments at the same time, appointment time column **758** may be identified as not including identifiable information of a patient based on the distribution of appointment times in the column), may be based on values in the column (for example, a comparison of values in patient name column **752** with a dictionary may indicate that the values include names, and therefore patient name column **752** be identified as including identifiable information of a patient), may be based on analysis of values in the column and/or in other columns (for example using a machine learning model trained using training examples), and so forth.

In some embodiments, an identified copy of the data element and a de-identified copy of the data element may be used, for example as described below. For example, the identified copy of the data element may include identified information of a patient, and the de-identified copy of the data element may include no identified information of a patient. In the examples of FIG. 7B and FIG. 7C, any one of data element **730** and data element **750** includes identified information of a patient, and therefore data element **730** and data element **750** are identified copies. In one example, de-identified copies of data element **730** and data element **750** may include data fields that comprise no identified information of a patient and may exclude fields that comprise identified information of a patient. For example, a de-identified copy of data element **730** may include portion **744** of data element **730** and may not include any part of portion **742** of data element **730**. In another example, a de-identified copy of data element **730** may include data field **756** but not data fields **752** and **754**, and may include or not include data field **758** based on whether data field **758** includes identified information of a patient (for example, as determined as described above). In one example, the identified copy and/or the de-identified copy may be obtained by accessing the identified copy and/or the de-identified copy in a memory (such as memory units **210**, shared memory modules **410**, and so forth). In another example, the identified copy and/or the de-identified copy may be received from an external device over a communication network using a communication device (such as communication modules **230**, internal communication modules **440**, external communication modules **450**, etc.), may be received from a user, and so forth. In some examples, the identified copy may be analyzed to generate the de-identified copy. For example, a machine learning model may be trained using training example to generate de-identified copies of data sources that includes identified information, and the trained

machine learning model may be used to analyze a data element and generate a de-identified copy of data element. An example of such training example may include a sample data element together with a desired de-identified copy of the sample data element. In another example, the identified copy may include a plurality of fields, for each field it may be determined whether the field includes identified information of a patient (for example as described above), and fields that are determined to not include identified information of a patient may be included in the de-identified copy, while fields that are determined to include identified information of a patient may be omitted from the de-identified copy.

In some embodiments, a method, such as methods **800**, **820**, **830**, **840**, **860**, **880**, **900**, **920**, **930**, **940**, **950**, **960**, **1000**, **1100**, **1200**, **1300**, etc., may comprise of one or more steps. In some examples, a method, as well as all individual steps therein, may be performed by various aspects of computing device **200**, cloud platform **400**, computational node **500**, and so forth. For example, the method may be performed by processing units **220** executing software instructions stored within memory units **210** and/or within shared memory modules **410**. In some examples, a method, as well as all individual steps therein, may be performed by a dedicated hardware. In some examples, computer readable medium (such as a non-transitory computer readable medium) may store data and/or computer implementable instructions for carrying out a method. Some examples of possible execution manners of a method may include continuous execution (for example, returning to the beginning of the method once the method normal execution ends), periodically execution, executing the method at selected times, execution upon the detection of a trigger (some examples of such trigger may include a trigger from a user, a trigger from another method, a trigger from an external device, etc.), and so forth.

In some embodiments, machine learning algorithms (also referred to as machine learning models in the present disclosure) may be trained using training examples, for example in the cases described below. Some examples of such machine learning algorithms may include classification algorithms, data regressions algorithms, image segmentation algorithms, visual detection algorithms (such as object detectors, face detectors, person detectors, motion detectors, edge detectors, etc.), visual recognition algorithms (such as face recognition, person recognition, object recognition, etc.), speech recognition algorithms, mathematical embedding algorithms, natural language processing algorithms, support vector machines, random forests, nearest neighbors algorithms, deep learning algorithms, artificial neural network algorithms, convolutional neural network algorithms, recursive neural network algorithms, linear algorithms, non-linear algorithms, ensemble algorithms, and so forth. For example, a trained machine learning algorithm may comprise an inference model, such as a predictive model, a classification model, a regression model, a clustering model, a segmentation model, an artificial neural network (such as a deep neural network, a convolutional neural network, a recursive neural network, etc.), a random forest, a support vector machine, and so forth. In some examples, the training examples may include example inputs together with the desired outputs corresponding to the example inputs. Further, in some examples, training machine learning algorithms using the training examples may generate a trained machine learning algorithm, and the trained machine learning algorithm may be used to estimate outputs for inputs not included in the training examples. In some examples, engineers, scientists, processes and machines that train machine learning algorithms may further use validation examples

and/or test examples. For example, validation examples and/or test examples may include example inputs together with the desired outputs corresponding to the example inputs, a trained machine learning algorithm and/or an intermediately trained machine learning algorithm may be used to estimate outputs for the example inputs of the validation examples and/or test examples, the estimated outputs may be compared to the corresponding desired outputs, and the trained machine learning algorithm and/or the intermediately trained machine learning algorithm may be evaluated based on a result of the comparison. In some examples, a machine learning algorithm may have parameters and hyper parameters, where the hyper parameters are set manually by a person or automatically by a process external to the machine learning algorithm (such as a hyper parameter search algorithm), and the parameters of the machine learning algorithm are set by the machine learning algorithm according to the training examples. In some implementations, the hyper-parameters are set according to the training examples and the validation examples, and the parameters are set according to the training examples and the selected hyper-parameters.

In some embodiments, trained machine learning algorithms (also referred to as trained machine learning models in the present disclosure) may be used to analyze inputs and generate outputs, for example in the cases described below. In some examples, a trained machine learning algorithm may be used as an inference model that when provided with an input generates an inferred output. For example, a trained machine learning algorithm may include a classification algorithm, the input may include a sample, and the inferred output may include a classification of the sample (such as an inferred label, an inferred tag, and so forth). In another example, a trained machine learning algorithm may include a regression model, the input may include a sample, and the inferred output may include an inferred value for the sample. In yet another example, a trained machine learning algorithm may include a clustering model, the input may include a sample, and the inferred output may include an assignment of the sample to at least one cluster. In an additional example, a trained machine learning algorithm may include a classification algorithm, the input may include an image, and the inferred output may include a classification of an item depicted in the image. In yet another example, a trained machine learning algorithm may include a regression model, the input may include an image, and the inferred output may include an inferred value for an item depicted in the image (such as an estimated property of the item, such as size, volume, age of a person depicted in the image, cost of a product depicted in the image, and so forth). In an additional example, a trained machine learning algorithm may include an image segmentation model, the input may include an image, and the inferred output may include a segmentation of the image. In yet another example, a trained machine learning algorithm may include an object detector, the input may include an image, and the inferred output may include one or more detected objects in the image and/or one or more locations of objects within the image. In some examples, the trained machine learning algorithm may include one or more formulas and/or one or more functions and/or one or more rules and/or one or more procedures, the input may be used as input to the formulas and/or functions and/or rules and/or procedures, and the inferred output may be based on the outputs of the formulas and/or functions and/or rules and/or procedures (for example, selecting one of the outputs of the formulas and/or functions and/or rules

and/or procedures, using a statistical measure of the outputs of the formulas and/or functions and/or rules and/or procedures, and so forth).

In some embodiments, artificial neural networks may be configured to analyze inputs and generate corresponding outputs. Some examples of such artificial neural networks may comprise shallow artificial neural networks, deep artificial neural networks, feedback artificial neural networks, feed forward artificial neural networks, autoencoder artificial neural networks, probabilistic artificial neural networks, time delay artificial neural networks, convolutional artificial neural networks, recurrent artificial neural networks, long short term memory artificial neural networks, and so forth. In some examples, an artificial neural network may be configured manually. For example, a structure of the artificial neural network may be selected manually, a type of an artificial neuron of the artificial neural network may be selected manually, a parameter of the artificial neural network (such as a parameter of an artificial neuron of the artificial neural network) may be selected manually, and so forth. In some examples, an artificial neural network may be configured using a machine learning algorithm. For example, a user may select hyper-parameters for the an artificial neural network and/or the machine learning algorithm, and the machine learning algorithm may use the hyper-parameters and training examples to determine the parameters of the artificial neural network, for example using back propagation, using gradient descent, using stochastic gradient descent, using mini-batch gradient descent, and so forth. In some examples, an artificial neural network may be created from two or more other artificial neural networks by combining the two or more other artificial neural networks into a single artificial neural network.

FIG. 8A illustrates an example of a method 800 for enabling graphical illustration based on private medical information. In this example, method 800 may comprise: receiving a subgroup defining input (Step 802), the subgroup defining input may define a subgroup of a group of patients; receiving a statistical query about the subgroup of the group of patients (Step 804); determine a size of the subgroup of the group of patients (Step 806); comparing the determined size of the subgroup of the group of patients with a selected subgroup size threshold (Step 808); in response to the determined size of the subgroup of the group of patients being larger than the selected subgroup size threshold, providing first information (Step 810), the first information may be based on the statistical query and configured to enable a presentation of a graphical illustration of an estimated property of the subgroup of the group of patients; and in response to the determined size of the subgroup of the group of patients being smaller than the selected subgroup size threshold, forgoing providing the first information (Step 812). In some implementations, method 800 may comprise one or more additional steps, while some of the steps listed above may be modified or excluded. For example, in some cases Step 802 and/or Step 804 and/or Step 806 and/or Step 808 and/or Step 810 and/or Step 812 may be excluded from method 800. In some implementations, one or more steps illustrated in FIG. 8A may be executed in a different order and/or one or more groups of steps may be executed simultaneously and/or a plurality of steps may be combined into single step and/or a single step may be broken down to a plurality of steps. In some examples, after completion of Step 810 and/or Step 812, method 800 may continue to execute method 840 and/or method 860. In some examples, after completion of Step 810, method 800 may continue to

execute method **880**. In some examples, after completion of Step **812**, method **800** may continue to execute method **830**.

In some embodiments, Step **802** may comprise receiving a subgroup defining input, where the subgroup defining input may define a subgroup of a group of patients. In some examples, the subgroup defining input may be based on a first input from a user, such as user **146**. For example, Step **802** may read at least part of the subgroup defining input from memory (such as memory units **210**, shared memory modules **410**, and so forth). In another example, Step **802** may receive at least part of the subgroup defining input from an external device (such as computerized data analysis device **144**, an external device associated with the user, such as a workstation, a mobile device of the user, etc.) over a communication network using a communication device (such as communication modules **230**, internal communication modules **440**, external communication modules **450**, etc.), may receive at least part of the subgroup defining input from the user (for example, through a user interface, through a web page, using an input device, through computerized data analysis device **144**, etc.), and so forth. In one example, the subgroup defining input received by Step **802** may include a query (for example, in a query language such as Structured Query Language) that selects patients of the group of patients to the subgroup of a group of patients. In another example, the subgroup defining input received by Step **802** may include one or more criteria that dictate which patients of the group of patients are included in the subgroup of a group of patients. Some examples on such criteria may include restrictions on the age of the patients (for example, 'patients between the ages of 30 and 40'), restrictions on the gender of the patients (for example, 'female patients'), restrictions on physical characteristics of the patients (for example, 'patients with Body Mass Index under 20'), restriction on ethnicity of the patients (for example, 'Alaskan native patients'), restrictions on demographics of the patients (for example, 'patients with at least two children', 'patients with twelve or more years of education', 'patients with an annual income of at least \$30,000', etc.), restrictions on symptoms experienced by the patients (for example, 'patients suffering from back pain'), restrictions on the medical condition of the patients (for example, 'patients suffering from psychiatric disorders'), restriction on durations of medical conditions of the patients (for example, 'patients suffering from fibromyalgia for over a year'), restrictions on the medical treatment received by the patients (for example, 'patients received neuroleptic medication', 'patients who underwent corrective laser eye surgery', etc.), restrictions on adverse effects reported by the patients, restrictions on the medical examinations performed on the patients (for example, 'patients who underwent colonoscopy in the last year'), restrictions on a medical outcome associated with the patients (for example, 'patients with at least one hospital readmission'), restrictions on caregivers of the patients (for example, 'patients treated in a community clinic'), and so forth.

In some embodiments, Step **804** may comprise receiving a statistical query about a subgroup of the group of patients, for example receiving a statistical query about the subgroup of the group of patients defined by the subgroup defining input of Step **802**. In some examples, the statistical query may be based on an input from a user (for example, based on a second input from the user of Step **802**, based on an input from user **146**, based on an input from user **147**, and so forth). For example, Step **804** may read at least part of the statistical query about the subgroup of the group of patients from memory (such as memory units **210**, shared memory

modules **410**, and so forth). In another example, Step **804** may receive at least part of the statistical query about the subgroup of the group of patients from an external device (such as computerized data analysis device **144**, an external device associated with the user, such as a workstation, a mobile device of the user, etc.) over a communication network using a communication device (such as communication modules **230**, internal communication modules **440**, external communication modules **450**, etc.), may receive at least part of the statistical query about the subgroup of the group of patients from the user (for example, through a user interface, through a web page, using an input device, through computerized data analysis device **144**, etc.), and so forth. In one example, the statistical query about the subgroup of the group of patients received by Step **804** may include a query in a query language (such as Structured Query Language) that expresses a statistical query about the subgroup of the group of patients. In another example, the statistical query about the subgroup of the group of patients received by Step **804** may include one or more mathematical formulas for calculating a statistical measure of the subgroup of the group of patients.

In some embodiments, Step **806** may comprise determining a size of a subgroup of a group of patients, for example determining a size of the subgroup of the group of patients defined by the subgroup defining input of Step **802**, or determining a size of the updated subgroup of the group of patients of method **840** (described below). For example, Step **806** may determine an exact size of the subgroup of the group of patients, Step **806** may determine an estimated size of the subgroup of the group of patients, and so forth. In one example, Step **806** may count the patients in the subgroup of the group of patients, for example by determining for each patient in the group of patients whether that patient is in the subgroup of the group of patients using the subgroup defining input of Step **802**, and the size of the subgroup of the group of patients determined by Step **806** may be the determined number of patients in the subgroup of the group of patients. In another example, Step **806** may estimate the size of the subgroup of the group of patients, for example by determining for each patient in a selected sample of the group of patients whether that patient is in the subgroup of the group of patients using the subgroup defining input of Step **802** to estimate the ratio of patients in the subgroup of the group of patients from the entire group of patients, and using the estimated ratio and a known size of the group of patients to estimate the size of the subgroup of the group of patients. In some examples, a weight may be associated with each patient in the group of patients, and Step **806** may determine a total weight (exact total weight and/or estimated total weight) of the patients in the subgroup of the group of patients, and the size of the subgroup of the group of patients determined by Step **806** may be the determined total weight.

In some embodiments, Step **808** may comprise comparing a size of a subgroup of the group of patients (for example, the size determined by Step **806** of the subgroup of the group of patients defined by the subgroup defining input of Step **802**) with a selected subgroup size threshold. For example, Step **808** may read the subgroup size threshold from memory (such as memory units **210**, shared memory modules **410**, and so forth). In another example, Step **808** may receive the subgroup size threshold from an external device over a communication network using a communication device (such as communication modules **230**, internal communication modules **440**, external communication modules **450**, and so forth). In yet another example, Step **808** may receive the subgroup size threshold from a user (for

25

example, through a user interface, through a web page, using an input device, and so forth). In an additional example, Step 808 may receive the subgroup size threshold as a configuration parameter, for example from a configuration file. In some examples, Step 808 may randomly select the subgroup size threshold from a distribution of thresholds. Some examples of such distribution of thresholds may include discrete distribution, continuous distribution, uniform distribution, binomial distribution, normal distribution, Bernoulli distribution, Poisson distribution, exponential distribution, Polya-Eggenberger distribution, zeta distribution, and so forth. In some examples, Step 808 may select the subgroup size threshold based on whether particular patients are included in the subgroup of the group of patients. For example, in response to the subgroup of the group of patients including a first patient, Step 808 may select a first value for the subgroup size threshold, and in response to the subgroup of the group of patients not including the first patient, Step 808 may select a second value for the subgroup size threshold (the second value differs from the first value). In another example, in response to the subgroup of the group of patients including at least a selected number of patients of a first type, Step 808 may select a first value for the subgroup size threshold, and in response to the subgroup of the group of patients not including at least the selected number of patients of the first type, Step 808 may select a second value for the subgroup size threshold (the second value differs from the first value). For example, the selected number of patients may be one, two, between three and five, above five, and so forth. In another example, Step 808 may select the selected number of patients based on at least one of the first type, the determined size of the subgroup of the group of patients, the size of the group of patients, and so forth. In some examples, Step 808 may select the subgroup size threshold based on a type of the property of the subgroup of the group of patients. For example, in response to the property of the subgroup of the group of patients being of a first type, Step 808 may select a first value for the subgroup size threshold, and in response to the property of the subgroup of the group of patients being of a second type, Step 808 may select a second value for the subgroup size threshold (the second value differs from the first value). In some examples, Step 808 may select the subgroup size threshold based on the user of Step 802. For example, in response to a first user, Step 808 may select a first value for the subgroup size threshold, and in response to a second user, Step 808 may select a second value for the subgroup size threshold (the second value differs from the first value). In another example, Step 808 may select the subgroup size threshold based on at least one of an identity of the user, a type of the user, an identity of a group of at least two users that includes the user, past behavior of the user, at least one previous statistical query that is based on an input from the user, information provided in response to at least one previous statistical query that is based on an input from the user, and so forth. In some examples, Step 808 may select the subgroup size threshold based on at least one previous statistical query about the subgroup of the group of patients. For example, in response to the previous statistical queries about the subgroup of the group of patients including a first statistical query, Step 808 may select a first value for the subgroup size threshold, and in response to the previous statistical queries about the subgroup of the group of patients not including the first statistical query, Step 808 may select a second value for the subgroup size threshold (the second value differs from the first value). In another example, Step 808 may select the subgroup size threshold based on information provided in

26

response to at least one previous statistical query about the subgroup of the group of patients. For example, in response to the information provided in response to at least one previous statistical query having a first property, Step 808 may select a first value for the subgroup size threshold, and in response to at least one previous statistical query not having the first property, Step 808 may select a second value for the subgroup size threshold (the second value differs from the first value).

In some embodiments, Step 810 may comprise providing first information, for example in response to the size determined by Step 806 of the subgroup of the group of patients defined by the subgroup defining input of Step 802 being larger than the selected subgroup size threshold of Step 808.

In some examples, the first information may be based on a statistical query (for example, on the statistical query received by Step 804). In some examples, the first information may be configured to enable a presentation of a graphical illustration of an estimated property of a subgroup of the group of patients (for example, of an estimated property of the subgroup of the group of patients defined by the subgroup defining input of Step 802), for example in response to the second input from the user of Step 804. For example, Step 810 may store the first information in memory (such as memory 700, memory units 210, memory modules 410, etc.), in storage device (such as local storage, remote storage, network attached storage, etc.), and so forth. In another example, Step 810 may transmit the first information to an external device, for example over a communication network using a communication device (such as communication modules 230, internal communication modules 440, external communication modules 450, and so forth). In some examples, Step 810 may present the first information to a user, for example through a user interface, through a web page, using an output device (such as a display screen, an augmented reality display system, a printer, a LED indicator, etc.), through computerized data analysis device 144, and so forth.

In some embodiments, Step 812 may comprise forgoing and/or withholding providing the first information of Step 810, for example in response to the size determined by Step 806 of the subgroup of the group of patients defined by the subgroup defining input of Step 802 being smaller than the selected subgroup size threshold of Step 808.

In some examples, provided information (such as the first information provided by Step 810 or Step 834, the second information provided by Step 848, Step 868 or Step 888, the first estimated property of the medical data provided by Step 904, the second estimated property of the medical data provided by Step 912 or by Step 934 or by Step 952, and so forth) may be based on a statistical query (such as the statistical query received by Step 804, the second statistical query received by Step 884, the first statistical query received by Step 902, the second statistical query received by Step 906, and so forth). For example, the first information provided by Step 810 or Step 834 may be based on the statistical query received by Step 804, the second information provided by Step 848 or Step 868 may be based on the statistical query received by Step 804, the second information provided by Step 888 may be based on the second statistical query received by Step 884, the first estimated property of the medical data provided by Step 904 may be based on the first statistical query received by Step 902, the second estimated property of the medical data provided by Step 912 or by Step 934 or by Step 952 may be based on the second statistical query received by Step 906, and so forth. In some examples, the provided information may include

information generated using the statistical query. For example, the statistical query may include a query in a query language (such as Structured Query Language), and the provided information may include a result of applying the included query to a database and/or a data structure, or include the result combined with some noise (for example, as generated using method **820** or using method **920**). In another example, the statistical query may include a mathematical formula, and the provided information may include a statistical measure of the subgroup of the group of patients and/or of the medical data calculated according to the included mathematical formula, or include the calculated statistical measure combined with some noise (for example, as generated using method **820** or using method **920**). In yet another example, information in private medical data **112** and/or memory **700** may be analyzed using the statistical query to determine the provided information.

In some examples, provided information (such as the first information provided by Step **810** or Step **834**, the second information provided by Step **848**, Step **868** or Step **888**, etc.) may be configured to enable and/or cause a presentation of a graphical illustration of an estimated property of a subgroup of the group of patients (for example, of an estimated property of the subgroup of the group of patients defined by the subgroup defining input of Step **802**, of an estimated property of the subgroup of the group of patients defined by the second subgroup defining input of Step **882**, etc.), for example in response to an input from the user (such as the second input from the user of Step **804**, the fourth input from the user of Step **884**, and so forth). For example, the estimated property of the subgroup of the group of patients may be an actual property of the subgroup of the group of patients. In another example, the estimated property of the subgroup of the group of patients may be an approximation of an actual property of the subgroup of the group of patients. In some examples, the property of the subgroup of the group of patients to be graphically illustrated may be selected based on the statistical query. For example, in response to a first statistical query, a first property of the subgroup of the group of patients may be graphically illustrated, and in response to a second statistical query, a second property of the subgroup of the group of patients may be graphically illustrated (the second property differs from the first property). Some non-limiting examples of such properties of the subgroup of the group of patients may include a distribution of data associated with the patients in the subgroup of the group of patients, distribution of ages of patients in the subgroup of the group of patients, distribution of genders of patients in the subgroup of the group of patients, distribution of physical characteristics of patients in the subgroup of the group of patients, distribution of ethnicity of patients in the subgroup of the group of patients, distribution of demographic properties of patients in the subgroup of the group of patients, distribution of symptoms experienced by patients in the subgroup of the group of patients, distribution of medical conditions of patients in the subgroup of the group of patients, distribution of durations of medical conditions of patients in the subgroup of the group of patients, distribution of medical treatment received by patients in the subgroup of the group of patients, distribution of adverse effects reported by patients in the subgroup of the group of patients, distribution of medical outcome associated with patients in the subgroup of the group of patients, distribution of properties of caregivers of patients in the subgroup of the group of patients, and so forth.

In some examples, the graphical illustration may include an image. For example, the image may be based on the images associated with the patients of the subgroup of the group of patients. In some examples, each patient of the subgroup of the group of patients may be associated with a medical image, and the graphical illustration may include a display of an image based on the images associated with the patients of the subgroup of the group of patients. Some non-limiting examples of such medical images may include x-rays, computed tomography images, ultrasound images, magnetic resonance images, positron-emission tomography images, color images (for example, of a skin feature, of a medical operation, etc.), images of biopsies, and so forth. For example, the displayed image may be an average image of the images associated with the patients of the subgroup of the group of patients. In another example, the displayed image may be a weighted sum of the images associated with the patients of the subgroup of the group of patients. In yet another example, the displayed image may be a function of the images associated with the patients of the subgroup of the group of patients. In an additional example, at least one pixel of the displayed image may be a weighted sum of a group of pixels, and the group of pixels may comprise at least one pixel from each image of the images associated with the patients of the subgroup of the group of patients. In yet another example, at least one pixel of the displayed image may be a function of a group of pixels, the group of pixels may comprise at least one pixel from each image of the images associated with the patients of the subgroup of the group of patients.

In some examples, the graphical illustration may include a visualization of a correlation matrix. In one example, the graphical illustration may include a visualization of a correlation matrix between survival probabilities of patients of the subgroup of the group of patients and treatment choices associated with the patients of the subgroup of the group of patients. In another example, the graphical illustration may include a visualization of a correlation matrix between outcome associated with patients of the subgroup of the group of patients and demographic characteristics of the patients of the subgroup of the group of patients. In some examples, the graphical illustration may include a visualization of a correlation tensor. For example, the graphical illustration may include a visualization of a correlation tensor visualizing relations among data elements associated with patients of the subgroup of the group of patients.

In some examples, the graphical illustration may include a visualization of correlations between data elements associated with patients of the subgroup of the group of patients. For example, the visualization of the correlations between the data elements may include one or more charts. Some non-limiting examples of such charts may include a bar chart, a plot chart, a line chart, an area chart, a scatter plot, a bubble chart, a column chart, a surface chart, a radar chart, a combo chart, and so forth.

In some examples, the graphical illustration may include a visualization of a distribution of patients with respect to a characteristic of the patients. Some non-limiting examples of such charts may include a pie chart, a donut chart, a histogram, and so forth.

FIG. **8B** illustrates an example of a method **820** for determining an estimated property of a subgroup of a group of patients. In this example, method **820** may comprise: obtaining a privacy parameter (Step **822**); selecting at least one noise value based on the obtained privacy parameter (Step **824**); and combining the at least one noise value with an actual property of a subgroup of a group of patients to

determine the estimated property of the subgroup of the group of patients (Step 826). In some implementations, method 820 may comprise one or more additional steps, while some of the steps listed above may be modified or excluded. For example, in some cases Step 822 and/or Step 824 and/or Step 826 may be excluded from method 820. In some implementations, one or more steps illustrated in FIG. 8B may be executed in a different order and/or one or more groups of steps may be executed simultaneously and/or a plurality of steps may be combined into single step and/or a single step may be broken down to a plurality of steps.

In some embodiments, Step 822 may comprise obtaining a privacy parameter. For example, the obtained privacy parameter may comprise at least one of a number, a seed to a pseudo-random number generator, a selection of a noise model, a type of noise distribution, a parameter of a noise distribution, an amount of randomness, and so forth. For example, Step 822 may read at least part of the privacy parameter from memory (such as memory units 210, shared memory modules 410, and so forth). In another example, Step 822 may receive at least part of the privacy parameter from an external device (such as computerized data analysis device 144, an external device associated with the user, such as a workstation, a mobile device of the user, etc.) over a communication network using a communication device (such as communication modules 230, internal communication modules 440, external communication modules 450, and so forth). In yet another example, Step 822 may receive at least part of the privacy parameter from a user (for example, through a user interface, through a web page, using an input device, and so forth). In an additional example, Step 822 may receive at least part of the privacy parameter as a configuration parameter, for example from a configuration file. In some examples, Step 822 may randomly select the privacy parameter from a distribution of privacy parameters. Some examples of such distribution of privacy parameters may include discrete distribution, continuous distribution, uniform distribution, binomial distribution, normal distribution, Bernoulli distribution, Poisson distribution, exponential distribution, Polya-Eggenberger distribution, zeta distribution, and so forth. In some examples, Step 822 may select the privacy parameter based on a size of the subgroup of the group of patients, for example based on the size of the subgroup of the group of patients determined by Step 806. For example, in response to a first determined size of the subgroup of the group of patients, Step 822 may select a first value for the privacy parameter, and in response to a second determined size of the subgroup of the group of patients, Step 822 may select a second value for the privacy parameter (the second value differs from the first value). In some examples, Step 822 may select the privacy parameter based on whether particular patients are included in the subgroup of the group of patients. For example, in response to the subgroup of the group of patients including a first patient, Step 822 may select a first value for the privacy parameter, and in response to the subgroup of the group of patients not including the first patient, Step 822 may select a second value for the privacy parameter (the second value differs from the first value). In another example, in response to the subgroup of the group of patients including at least a selected number of patients of a first type, Step 822 may select a first value for the privacy parameter, and in response to the subgroup of the group of patients not including at least the selected number of patients of the first type, Step 822 may select a second value for the privacy parameter (the second value differs from the first value). For example, the selected number of patients may be one, two, between three

and five, above five, and so forth. In another example, Step 822 may select the selected number of patients based on at least one of the first type, the determined size of the subgroup of the group of patients, the size of the group of patients, and so forth. In some examples, Step 822 may select the privacy parameter based on a type of the property of the subgroup of the group of patients. For example, in response to the property of the subgroup of the group of patients being of a first type, Step 822 may select a first value for the privacy parameter, and in response to the property of the subgroup of the group of patients being of a second type, Step 822 may select a second value for the privacy parameter (the second value differs from the first value). In some examples, Step 822 may select the privacy parameter based on the user of Step 802. For example, in response to a first user, Step 822 may select a first value for the privacy parameter, and in response to a second user, Step 822 may select a second value for the privacy parameter (the second value differs from the first value). In another example, Step 822 may select the privacy parameter based on at least one of an identity of the user, a type of the user, an identity of a group of at least two users that includes the user, past behavior of the user, at least one previous statistical query that is based on an input from the user, information provided in response to at least one previous statistical query that is based on an input from the user, and so forth. In some examples, Step 822 may select the privacy parameter based on at least one previous statistical query about the subgroup of the group of patients. For example, in response to the previous statistical queries about the subgroup of the group of patients including a first statistical query, Step 822 may select a first value for the privacy parameter, and in response to the previous statistical queries about the subgroup of the group of patients not including the first statistical query, Step 822 may select a second value for the privacy parameter (the second value differs from the first value). In another example, Step 822 may select the privacy parameter based on information provided in response to at least one previous statistical query about the subgroup of the group of patients. For example, in response to the information provided in response to at least one previous statistical query having a first property, Step 822 may select a first value for the privacy parameter, and in response to at least one previous statistical query not having the first property, Step 822 may select a second value for the privacy parameter (the second value differs from the first value).

In some embodiments, Step 824 may comprise selecting at least one noise value based on the privacy parameter obtained by Step 822. For example, Step 824 may obtain one or more noise values from a pseudo-random number generator initialized based on the privacy parameter obtained by Step 822 (for example, initialized using a seed included in the privacy parameter). In another example, Step 824 may obtain one or more noise values from a noise model selected from a plurality of alternative noise models based on the privacy parameter obtained by Step 822 (for example, according to an indication of a selected noise model included in the privacy parameter). In yet another example, Step 824 may obtain one or more noise values from a noise distribution, and the type and/or at least part of parameters of the noise distribution may be selected based on the privacy parameter obtained by Step 822 (for example, according to an indication of a type of a noise distribution included in the privacy parameter, according to a parameter of the noise distribution included in the privacy parameter, and so forth). In an additional example, Step 824 may obtain one or more noise values from a list of previously generated

random values (for example, the selection of the one or more noise values from the list may be based on the privacy parameter obtained by Step 822). In some examples, the amount of noise values selected by Step 824 may be controlled according to the privacy parameter obtained by Step 822 (for example, according to an amount of randomness specified in the privacy parameter obtained by Step 822).

In some embodiments, Step 826 may combine at least one noise value with an actual property of a subgroup of a group of patients to determine an estimated property of the subgroup of the group of patients. For example, Step 826 may combine the at least one noise value selected by Step 824 with an actual property of the subgroup of the group of patients defined by the subgroup defining input of Step 802 to determine the estimated property of the subgroup of the group of patients. For example, the actual property of the subgroup of the group of patients may include a number, and Step 826 may manipulate the number using a noise value (for example, adding the noise value to the number, multiplying the number by the noise value, etc.) to obtain the estimated property of the subgroup of the group of patients. In another example, the actual property of the subgroup of the group of patients may include a list of details, and Step 826 may manipulate the list of details using the at least one noise value (for example, dropping at least part of the items in the list of details based on the at least one noise value, adding items to the list of details based on the at least one noise value, modifying items in the list of details based on the at least one noise value, switching the order of the items in the list of details based on the at least one noise value, etc.) to obtain the estimated property of the subgroup of the group of patients.

FIG. 8C illustrates an example of a method 830 for enabling graphical illustration based on private medical information. In this example, method 830 may comprise: receiving an indication that an update to a status of the user occurred (Step 832), for example after forgoing providing the first information by Step 812; and in response to the update to the status of the user, providing the first information (Step 834). In some implementations, method 830 may comprise one or more additional steps, while some of the steps listed above may be modified or excluded. For example, in some cases Step 832 and/or Step 834 may be excluded from method 830. In some implementations, one or more steps illustrated in FIG. 8C may be executed in a different order and/or one or more groups of steps may be executed simultaneously and/or a plurality of steps may be combined into single step and/or a single step may be broken down to a plurality of steps. In some examples, method 830 and/or Step 832 may be executed after forgoing providing the first information by Step 812 of method 800.

In some embodiments, Step 832 may comprise receiving an indication that an update to a status of the user of Step 802 occurred, for example after forgoing providing the first information by Step 812 of method 800. For example, Step 832 may receive the indication from a permissions system and/or a permissions database (such as permissions 716), from a repository of regulatory statuses of users, from regulators (such as regulators 650), from a repository of user information, from a repository of employment records (for example, employment records of the user, employment records of medical care providers 630, employment records of insurers 640, employment records of regulators 650, employment records of researchers 660, employment records of facilitators 670, employment records of medical organization 110A, employment records of team 140A, etc.),

and so forth. In one example, Step 832 may read the indication from memory (such as memory units 210, shared memory modules 410, and so forth). In another example, Step 832 may receive the indication from an external device over a communication network using a communication device (such as communication modules 230, internal communication modules 440, external communication modules 450, and so forth). In yet another example, Step 832 may receive the indication from a user (for example, through a user interface, through a web page, using an input device, and so forth).

In some embodiments, Step 834 may comprise providing the first information in response to the update to the status of the user. For example, in response to a first update to the status of the user, Step 834 may provide the first information, and in response to a second update to the status of the user, Step 834 may forgo providing the first information. Step 834 may provide the first information as described above in relation to Step 810.

In some examples, the new status of the user may include a new permission, Step 832 may receive an indication that an update to the permissions of the user of Step 802 occurred, and Step 834 may provide the first information in response to the new permission of the user. For example, in response to a first new permission of the user, Step 834 may provide the first information, and in response to a second new permission of the user, Step 834 may forgo providing the first information.

In some examples, the new status of the user may include an approval of an Institutional Review Board for the user to use at least some information, Step 832 may receive an indication that an update to the approvals of the Institutional Review Board for the user of Step 802 occurred, and Step 834 may provide the first information in response to the new approval for the user. For example, in response to a first new approval for the user, Step 834 may provide the first information, and in response to a second new approval for the user, Step 834 may forgo providing the first information.

In some examples, the new status of the user may include a new employment status, Step 832 may receive an indication that an update to the employment status of the user of Step 802 occurred, and Step 834 may provide the first information in response to the new employment status of the user. For example, in response to a first new employment status of the user, Step 834 may provide the first information, and in response to a second new employment status of the user, Step 834 may forgo providing the first information.

FIG. 8D illustrates an example of a method 840 for enabling graphical illustration based on private medical information. In this example, method 840 may comprise: receiving an indication that an update to the group of patients caused an update to the subgroup defined by the subgroup defining input (Step 842); determining a size of the updated subgroup (Step 844); comparing the determined size of the updated subgroup with a selected second subgroup size threshold (Step 846); in response to the determined size of the subgroup of the group of patients being smaller than the selected subgroup size threshold and the determined size of the updated subgroup being larger than the selected second subgroup size threshold, providing second information (Step 848), the second information may be based on the statistical query and may be configured to enable a presentation of a graphical illustration of an estimated property of the updated subgroup; in response to the determined size of the subgroup of the group of patients being larger than the selected subgroup size threshold, forgoing providing the second information (Step 850); and

in response to the determined size of the updated subgroup being smaller than the selected second subgroup size threshold, forgoing providing the second information (Step 852). In some implementations, method 840 may comprise one or more additional steps, while some of the steps listed above may be modified or excluded. For example, in some cases Step 842 and/or Step 844 and/or Step 846 and/or Step 848 and/or Step 850 and/or Step 852 may be excluded from method 840. In some implementations, one or more steps illustrated in FIG. 8D may be executed in a different order and/or one or more groups of steps may be executed simultaneously and/or a plurality of steps may be combined into single step and/or a single step may be broken down to a plurality of steps. In some examples, method 840 and/or Step 842 may be executed after method 800.

In some embodiments, Step 842 may comprise receiving an indication that an update to the group of patients caused an update to the subgroup defined by the subgroup defining input of Step 802. For example, the group of patients may be patients 610, and Step 842 may receive an indication that an update to patients 610 caused an update to the subgroup defined by the subgroup defining input of Step 802. In another example, Step 842 may read the indication from memory (such as memory units 210, shared memory modules 410, and so forth). In another example, Step 842 may receive the indication from an external device over a communication network using a communication device (such as communication modules 230, internal communication modules 440, external communication modules 450, and so forth). In yet another example, Step 842 may receive the indication from a user (for example, through a user interface, through a web page, using an input device, and so forth). In one example, the updated subgroup of Step 842 may include at least one patient not included in the subgroup of the group of patients defined by the subgroup defining input of Step 802. In another example, the subgroup of the group of patients defined by the subgroup defining input of Step 802 may include at least one patient not included in the updated subgroup of Step 842. In some other examples, the size of the updated subgroup of Step 842 may be larger than the size of the subgroup of the group of patients defined by the subgroup defining input of Step 802, may be identical to the size of the subgroup of the group of patients defined by the subgroup defining input of Step 802, may be smaller than the size of the subgroup of the group of patients defined by the subgroup defining input of Step 802, may be different than the size of the subgroup of the group of patients defined by the subgroup defining input of Step 802, and so forth.

In some embodiments, Step 844 may comprise determining a size of the updated subgroup of Step 842, for example using Step 806 as described above.

In some embodiments, Step 846 may comprise comparing the size of the updated subgroup determined by Step 844 with a selected second subgroup size threshold. For example, the selected second subgroup size threshold may be identical to the selected subgroup size threshold of method 800, may be different from the selected subgroup size threshold of method 800, may be larger than the selected subgroup size threshold of method 800, may be smaller than the selected subgroup size threshold of method 800, and so forth. In some examples, Step 846 may select the second subgroup size threshold based on the selected subgroup size threshold of method 800. For example, in response to a first selected subgroup size threshold of method 800, Step 846 may select a first value for the second subgroup size threshold, and in response to a second selected subgroup size threshold of method 800, Step 846 may select a second value

for the second subgroup size threshold (the second value differs from the first value). In some examples, Step 846 may obtain and/or select the second subgroup size threshold in a similar fashion to the selection of the selected subgroup size threshold of method 800 by Step 808 described above.

In some embodiments, Step 848 may comprise providing second information, for example in response to the size of the subgroup of the group of patients of method 800 determined by Step 806 being smaller than the selected subgroup size threshold of Step 808 and the size of the updated subgroup determined by Step 844 being larger than the selected second subgroup size threshold of Step 846. In some examples, the second information may be based on a statistical query (for example, on the statistical query of method 800). In some examples, the second information may be configured to enable a presentation of a graphical illustration of an estimated property of the updated subgroup of Step 842, for example to the user of method 800. For example, Step 848 may provide the second information in a similar fashion to the providence of the first information by Step 810 as described above. In some examples, the second information provided by Step 848 may be identical to the first information of method 800, may be different from the first information of method 800, and so forth.

In some embodiments, Step 850 may comprise forgoing and/or withholding providing the second information of Step 848, for example in response to the size of the subgroup of the group of patients of method 800 determined by Step 806 being larger than the selected subgroup size threshold of Step 808.

In some embodiments, Step 852 may comprise forgoing and/or withholding providing the second information of Step 848, for example in response to the size of the updated subgroup determined by Step 844 being smaller than the selected second subgroup size threshold of Step 846.

FIG. 8E illustrates an example of a method 860 for enabling graphical illustration based on private medical information. In this example, method 860 may comprise: receiving an indication that an update to the group of patients caused an update to the subgroup defined by the subgroup defining input (Step 842); determining a size of the updated subgroup (Step 844); comparing the determined size of the updated subgroup with a selected second subgroup size threshold (Step 846); in response to the determined size of the subgroup of the group of patients being larger than the selected subgroup size threshold and the determined size of the updated subgroup being larger than the selected second subgroup size threshold, providing second information (Step 868), the second information may be based on the statistical query and may be configured to enable a presentation of a graphical illustration of an estimated property of the updated subgroup; and in response to the determined size of the updated subgroup being smaller than the selected second subgroup size threshold, forgoing providing the second information (Step 870). In some implementations, method 860 may comprise one or more additional steps, while some of the steps listed above may be modified or excluded. For example, in some cases Step 842 and/or Step 844 and/or Step 846 and/or Step 868 and/or Step 870 may be excluded from method 860. In some implementations, one or more steps illustrated in FIG. 8E may be executed in a different order and/or one or more groups of steps may be executed simultaneously and/or a plurality of steps may be combined into single step and/or a single step may be broken down to a plurality of steps. In some

35

examples, method **860** and/or Step **862** may be executed after providing the first information by Step **810** of method **800**.

In some embodiments, Step **868** may comprise providing second information, for example in response to the determined size of the subgroup of the group of patients of method **800** determined by Step **806** being larger than the selected subgroup size threshold of Step **808** and the size of the updated subgroup determined by Step **844** being larger than the selected second subgroup size threshold of Step **846**. In some examples, the second information may be based on a statistical query (for example, on the statistical query of method **800**). In some examples, the second information may be configured to enable a presentation of a graphical illustration of an estimated property of the updated subgroup of Step **842**, for example to the user of method **800**. For example, Step **868** may provide the second information in a similar fashion to the providence of the first information by Step **810** as described above. In some examples, the second information provided by Step **868** may be identical to the first information of method **800**, may be different from the first information of method **800**, and so forth.

In some embodiments, Step **870** may comprise forgoing and/or withholding providing the second information of Step **868**, for example in response to the size of the updated subgroup determined by Step **844** being smaller than the selected second subgroup size threshold of Step **846**.

In some embodiments, method **860** may further comprise forgoing and/or withholding providing the second information of Step **868**, for example in response to the size of the subgroup of the group of patients of method **800** determined by Step **806** being smaller than the selected subgroup size threshold of Step **808**.

FIG. **8F** illustrates an example of a method **880** for enabling graphical illustration based on private medical information. In this example, method **880** may comprise: receiving a second subgroup defining input (Step **882**), for example after providing the first information, the second subgroup defining input may be based on a third input from the user and may define a second subgroup of the group of patients; receiving a second statistical query about the second subgroup of the group of patients (Step **884**), the second statistical query may be based on a fourth input from the user; determining a size of a difference between the subgroup of the group of patients and the second subgroup of the group of patients (Step **886**); in response to the determined size of the difference between the subgroup of the group of patients and the second subgroup of the group of patients being larger than a selected difference threshold, providing second information (Step **888**), the second information may be based on the second statistical query and may be configured to enable a presentation of a graphical illustration of an estimated property of the second subgroup of the group of patients, for example in response to the fourth input from the user; and in response to the determined size of the difference between the subgroup of the group of patients and the second subgroup of the group of patients being smaller than a selected difference threshold, forgoing providing the second information (Step **890**). In some implementations, method **880** may comprise one or more additional steps, while some of the steps listed above may be modified or excluded. For example, in some cases Step **882** and/or Step **884** and/or Step **886** and/or Step **888** and/or Step **890** may be excluded from method **880**. In some implementations, one or more steps illustrated in FIG. **8F** may be executed in a different order and/or one or more groups of

36

steps may be executed simultaneously and/or a plurality of steps may be combined into single step and/or a single step may be broken down to a plurality of steps. In some examples, method **880** and/or Step **882** may be executed after providing the first information by Step **810** of method **800**.

In some embodiments, Step **882** may comprise receiving a second subgroup defining input, for example, after providing the first information (for example using Step **810** or Step **834**), where the second subgroup defining input may define a second subgroup of the group of patients. In some examples, the second subgroup defining input may be based on an input from a user, such as a third input from the user of method **800**. In some examples, Step **882** may receive the second subgroup defining input in a similar fashion to the reception of the subgroup defining input by Step **802** described above. In some examples, the structure of the second subgroup defining input may be similar or identical to the structure of the subgroup defining input of Step **802** described above.

In some embodiments, Step **884** may comprise receiving a second statistical query about the second subgroup of the group of patients defined by the second subgroup defining input of Step **882**. In some examples, the second statistical query may be based on an input from a user, such as a fourth input from the user of method **800**. In some examples, Step **884** may receive the second statistical query in a similar fashion to the reception of the statistical query by Step **804**. In some examples, the structure of the second statistical query may be similar or identical to the structure of the statistical query of Step **804** described above.

In some embodiments, Step **886** may comprise determining a size of a difference between the subgroup of the group of patients defined by the subgroup defining input of Step **802** and the second subgroup of the group of patients defined by the second subgroup defining input of Step **882**. For example, Step **886** may determine an exact size of the difference, an estimated size of the difference, and so forth. In one example, Step **886** may determine at least one of the number (and/or a total weight according to an assignment of weight to patients) of patients in the subgroup of the group of patients defined by the subgroup defining input of Step **802** that are not in the second subgroup of the group of patients defined by the second subgroup defining input of Step **882**, the number (and/or a total weight according to an assignment of weight to patients) of patients in the second subgroup of the group of patients defined by the second subgroup defining input of Step **882** that are not in the subgroup of the group of patients defined by the subgroup defining input of Step **802**, the number (and/or a total weight according to an assignment of weight to patients) of patients that are in both the subgroup of the group of patients defined by the subgroup defining input of Step **802** and the second subgroup of the group of patients defined by the second subgroup defining input of Step **882**. Further, in some examples, Step **886** may determine the size of the difference as a linear combination and/or a non-linear combination of one or more of the above determined numbers and/or above determined total weights. In some examples, any function that measures and/or estimates a difference and/or a distance between two mathematical sets may be used by Step **886** to determine the size of the difference.

In some embodiments, Step **888** may comprise providing second information, for example in response to the size of the difference between the subgroup of the group of patients and the second subgroup of the group of patients determined by Step **886** being larger than a selected difference threshold.

In some examples, the second information may be based on a statistical query (for example, on the second statistical query received by Step 884). In some examples, the second information may be configured to enable a presentation of a graphical illustration of an estimated property of the second subgroup of the group of patients defined by the second subgroup defining input of Step 882, for example in response to the fourth input from the user of Step 884. For example, Step 888 may provide the second information in a similar fashion to the providence of the first information by Step 810 as described above. In some examples, the second information provided by Step 888 may be identical to the first information of method 800, may be different from the first information of method 800, and so forth.

In some embodiments, Step 890 may comprise forgoing and/or withholding providing the second information of Step 888, for example in response to the size of the difference between the subgroup of the group of patients and the second subgroup of the group of patients determined by Step 886 being smaller than a selected difference threshold.

In some examples, the difference threshold of Step 888 and Step 890 may be selected by method 880. For example, the difference threshold may be read from memory (such as memory units 210, shared memory modules 410, and so forth). In another example, the difference threshold may be received from an external device over a communication network using a communication device (such as communication modules 230, internal communication modules 440, external communication modules 450, and so forth). In yet another example, the difference threshold may be received from a user (for example, through a user interface, through a web page, using an input device, and so forth). In an additional example, the difference threshold may be received as a configuration parameter, for example from a configuration file. In some examples, the difference threshold may be selected based on the selected subgroup size threshold of method 800. For example, in response to a first selected subgroup size threshold of method 800, a first value may be selected for the difference threshold, and in response to a second selected subgroup size threshold of method 800, a second value may be selected for the difference threshold (the second value differs from the first value). In some examples, the difference threshold may be selected in a similar fashion to the selection of the selected subgroup size threshold of method 800 by Step 808 described above. For example, the difference threshold may be randomly selected from a distribution of thresholds. In another example, the difference threshold may be selected based on at least one of whether the subgroup of the group of patients includes a first patient, whether the second subgroup of the group of patients includes a first patient, whether the subgroup of the group of patients includes at least a selected number of patients of a first type (wherein the selected number of patients is one, is two, is between three and five, is above five, and so forth), whether the second subgroup of the group of patients includes at least a selected number of patients of a first type (wherein the selected number of patients is one, is two, is between three and five, is above five, and so forth), the determined size of the subgroup of the group of patients, the size of the second subgroup of the group of patients, the size of the group of patients, a type of the property of the subgroup of the group of patients, a type of the property of the second subgroup of the group of patients, the user, an identity of the user, a type of the user, an identity of a group of at least two users that includes the user, past behavior of the user, at least one previous statistical query that is based on an input from the user, information provided in response

to at least one previous statistical query that is based on an input from the user, and so forth.

In some embodiments, a user (such as user 146) may use a computerized data analysis device (such as computerized data analysis device 144) to enter input (such as the first input from the user of Step 802, the second input from the user of Step 804, the third input from the user of Step 882, the fourth input from the user of Step 884, and so forth). The computerized data analysis device may generate a subgroup defining input (such as the subgroup defining input of Step 802, the second subgroup defining input of Step 882, etc.) and/or a statistical query (such as the statistical query received by Step 804, the second statistical query received by Step 884, and so forth) based on the input entered by the user. The computerized data analysis device may provide the generated subgroup defining input and/or statistical query to medical organization 110 (for example, to a computerized device within medical organization 110, to a software of medical organization 110 executed on cloud platform 400, etc.), for example by transmitting the generated subgroup defining input and/or statistical query through communication network 130. Medical organization 110 (for example, using a computerized device, using a software program, etc.) may use methods 800, 820, 830, 840, 860 and 880 to generate a response to the statistical query including information (such as the first information provided by Step 810 or Step 834, the second information provided by Step 848, Step 868 or Step 888, and so forth), and the generated response may be provided back to computerized data analysis device, for example by transmitting the generated response through communication network 130. Further, in some examples, the computerized data analysis device may receive the generated response, and present a graphical illustration of an estimated property of a subgroup of the group of patients (for example, of an estimated property of the subgroup of the group of patients defined by the subgroup defining input of Step 802, by the second subgroup defining input of Step 882, etc.), for example in response to the input entered by the user (for example, in response to the first input from the user of Step 802, to the second input from the user of Step 804, to the third input from the user of Step 882, to the fourth input from the user of Step 884, and so forth). In some examples, the graphical illustration may be further based on information from public data 120 and/or proprietary medical data 142. In some examples, the graphical illustration may be further based on information received from multiple medical organizations, such as medical organizations 110A, 110B and 110C. For example, each medical organization may provide information as described above, the provided information from the multiple medical organizations may be combined, and the graphical illustration may be based on the combined information.

FIG. 9A illustrates an example of a method 900 for selectively providing information about medical data. In this example, method 900 may comprise: receiving a first statistical query about medical data (Step 902), the first statistical query may be based on an input from a first user; providing a first estimated property of the medical data to the first user (Step 904), the first estimated property of the medical data may be based on the first statistical query; receiving a second statistical query about the medical data (Step 906), the second statistical query may be based on an input from a second user; selecting a first group of users that includes the first user (Step 908); determining whether the first group of users includes the second user (Step 910); in response to a determination that the first group of users does not include the second user, providing a second estimated

39

property of the medical data to the second user (Step 912), the second estimated property of the medical data may be based on the second statistical query; and in response to a determination that the first group of users includes the second user, forgoing providing the second estimated property of the medical data to the second user (Step 914). In some implementations, method 900 may comprise one or more additional steps, while some of the steps listed above may be modified or excluded. For example, in some cases Step 902 and/or Step 904 and/or Step 906 and/or Step 908 and/or Step 910 and/or Step 912 and/or Step 914 may be excluded from method 900. In some implementations, one or more steps illustrated in FIG. 9A may be executed in a different order and/or one or more groups of steps may be executed simultaneously and/or a plurality of steps may be combined into single step and/or a single step may be broken down to a plurality of steps. In some examples, after completion of Step 912, method 900 may continue to execute method 940. In some examples, after completion of Step 912, method 900 may continue to execute method 960. In some examples, after completion of Step 914, method 900 may continue to execute method 930.

In some embodiments, Step 902 may comprise receiving a first statistical query about medical data. In some examples, the first statistical query received by Step 902 may be based on an input from a first user (such as user 146). In some embodiments, Step 906 may comprise receiving a second statistical query about the medical data. In some examples, the second statistical query received by Step 906 may be based on an input from a second user (such as user 146, user 147, user 148, and so forth). In some examples, the second user may differ from the first user, the second user may be the first user, and so forth. In some embodiments, Step 902 and/or Step 906 may read at least part of the statistical query about the medical data from memory (such as memory units 210, shared memory modules 410, and so forth). In another example, Step 902 and/or Step 906 may receive at least part of the statistical query about the medical data from an external device (such as computerized data analysis device 144, an external device associated with the user, such as a workstation, a mobile device of the user, etc.) over a communication network using a communication device (such as communication modules 230, internal communication modules 440, external communication modules 450, etc.), may receive at least part of the statistical query about the medical data from the user (for example, through a user interface, through a web page, using an input device, through computerized data analysis device 144, etc.), and so forth. In one example, the statistical query about the medical data received by Step 902 and/or the statistical query about the medical data received by Step 906 may include a query in a query language (such as Structured Query Language) that expresses a statistical query about the medical data. In another example, the statistical query about the medical data received by Step 902 and/or the statistical query about the medical data received by Step 906 may include one or more mathematical formulas for calculating a statistical measure of the medical data.

In some embodiments, Step 904 may comprise providing a first estimated property of the medical data, for example to the first user of Step 902. In some examples, the first estimated property of the medical data may be based on a statistical query (for example, on the first statistical query received by Step 902). For example, Step 904 may store the first estimated property of the medical data in memory (such as memory 700, memory units 210, memory modules 410, etc.), in storage device (such as local storage, remote stor-

40

age, network attached storage, etc.), and so forth. In another example, Step 904 may transmit the first estimated property of the medical data to an external device, for example over a communication network using a communication device (such as communication modules 230, internal communication modules 440, external communication modules 450, and so forth). In some examples, Step 904 may present the first estimated property of the medical data to a user (such as the first user of Step 902), for example through a user interface, through a web page, using an output device (such as a display screen, an augmented reality display system, a printer, a LED indicator, etc.), through computerized data analysis device 144, and so forth. In one example, the first estimated property of the medical data provided by Step 904 may be an actual property of the medical data. In another example, the first estimated property of the medical data provided by Step 904 may be an approximation of an actual property of the medical data.

In some embodiments, Step 908 may comprise selecting a first group of users that includes the first user of Step 902. For example, the first group of users may include any number of users (such as one user, two users, between three and ten users, more than ten users, and so forth). In some examples, Step 908 may select the first group of users of a plurality of alternative groups of users. For example, Step 908 may select the first group of users of a plurality of alternative groups of users based on an identity of the first user of Step 902. In another example, a group of users that maximize a particular criterion function (such as, largest group, smallest group, etc.) from all the groups of users in the plurality of alternative groups of users that includes the first user may be selected. In some examples, the first group of users may be generated, for example by selecting users from a plurality of users according to a user selection rule. In some examples, the first group of users may be selected based on user input. For example, the user may specify the users in the first group of users, may select the first group of users from a plurality of alternative groups, may specify a user selection rule, and so forth. In some examples, the first group of users may be read from memory (such as memory units 210, shared memory modules 410, and so forth). In some examples, a type of the first user of Step 902 may be a particular type, and Step 908 may select the first group of users to include all users of the particular type from a particular plurality of users.

In some embodiments, Step 910 may comprise determining whether the first group of users selected by Step 908 includes the second user of Step 906. For example, a list of the users in the group of users may be accessed to determine whether the second user of Step 906 is in the list, and therefore determine whether the first group of users selected by Step 908 includes the second user of Step 906. In another example, a user selection rule defining which users are in the group of users may be used to determine whether the first group of users selected by Step 908 includes the second user of Step 906.

In some embodiments, Step 912 may comprise providing a second estimated property of the medical data, for example to the second user of Step 906, for example in response to a determination by Step 910 that the first group of users selected by Step 908 does not include the second user of Step 906. In some examples, the second estimated property of the medical data provided by Step 912 and/or Step 934 and/or Step 952 may be based on a statistical query (for example, on the second statistical query received by Step 906). For example, Step 912 and/or Step 934 and/or Step 952 may provide the second estimated property of the

41

medical data in a similar fashion to the providence of the first estimated property of the medical data by Step 904 described above. In one example, the second estimated property of the medical data provided by Step 912 and/or by Step 934 and/or by Step 952 may be an actual property of the medical data. In another example, the second estimated property of the medical data provided by Step 912 and/or by Step 934 and/or by Step 952 may be an approximation of an actual property of the medical data.

In some embodiments, Step 914 may comprise forgoing and/or withholding providing the second estimated property of the medical data of Step 912 to the second user of Step 906, for example in response to a determination by Step 910 that the first group of users selected by Step 908 includes the second user of Step 906.

Additionally or alternatively, in response to a determination that the first group of users includes the second user, Step 914 may cause a suggestion of an alternative statistical query to be provided to the second user of Step 906. In some examples, the alternative statistical query may be based on the second statistical query received by Step 906. For example, Step 914 may select the alternative statistical query from a plurality of possible statistical queries based on the second statistical query received by Step 906. In another example, Step 914 may use a function to transform the second statistical query received by Step 906 into the alternative statistical query. In some examples, Step 914 may provide a suggestion of the alternative statistical query to the second user, may cause an external device (such as computerized data analysis device 144) to provide the alternative statistical query to the second user (for example, by transmitting information configured to cause the external device to provide the alternative statistical query to the second user), and so forth. Further, in some examples, Step 914 may receive an indication that the second user of Step 906 accepted the suggested alternative statistical query. For example, Step 914 may receive user input from the second user indicating that the second user accepted the suggested alternative statistical query, may receive information from an external device (such as computerized data analysis device 144) indicating that the second user accepted the suggested alternative statistical query, and so forth. Further, in some examples, in response to the received indication that the second user accepted the suggested alternative statistical query, Step 914 may provide a third estimated property of the medical data to the second user. For example, the third estimated property of the medical data may be based on the suggested alternative statistical query. For example, Step 914 may provide the third estimated property of the medical data in a similar fashion to the providence of the first estimated property of the medical data by Step 904 described above.

In some embodiments, Step 904 may further comprise updating a privacy budget associated with the first group of users of Step 908 to reflect the providence of the first estimated property of the medical data to the first user of Step 902 by Step 904. For example, a first privacy consumption may be determined based on the first statistical query of Step 902 and/or based on the first estimated property of the medical data, and the privacy budget associated with the first group of users of Step 908 may be updated based on the determined first privacy consumption (for example, by reducing the first privacy consumption from the privacy budget, by multiplying the privacy budget by a factor selected based on the first privacy consumption, and so forth). For example, a machine learning model may be trained using training examples to determine privacy

42

consumption values from queries and/or provided information, and the trained machine learning model may be used to analyze the first statistical query of Step 902 and/or the first estimated property of the medical data to determine the first privacy consumption. An example of such training example may include a record of a query and/or of provided information, together with a label indicating the desired privacy consumption value to be determined.

Further, in some embodiments, Step 910 may further determine whether the updated privacy budget is sufficient for the second statistical query. For example, a projected privacy consumption may be determined based on the first statistical query of Step 906 and/or based on the second estimated property of the medical data to be provided by Step 912 (for example in a similar fashion to the determination of the first privacy consumption described above), and the updated privacy budget may be compared with the determined projected privacy consumption to determine whether the updated privacy budget is sufficient for the second statistical query.

Further, in some embodiments, in response to the determination by Step 910 that the first group of users selected by Step 908 includes the second user of Step 906 and a determination by Step 910 that the updated privacy budget is sufficient for the second statistical query of Step 906, the second estimated property of the medical data may be provided to the second user (for example as described above in relation to Step 912), and in response to the determination by Step 910 that the first group of users selected by Step 908 includes the second user of Step 906 and a determination by Step 910 that the updated privacy budget is insufficient for the second statistical query of Step 906, providing the second estimated property of the medical data to the second user may be withheld and/or forwent.

Further, in some embodiments, after Step 910 determines whether the updated privacy budget is sufficient for the second statistical query, a third statistical query about the medical data may be received. For example, the third statistical query may be based on an additional input from the first user. For example, the third statistical query about the medical data may be received using Step 962. Further, in some examples, in case the first group of users selected by Step 908 includes the second user of Step 906 and the second estimated property of the medical data was not provided to the second user, a third estimated property of the medical data may be provided to the first user (for example, the third estimated property of the medical data may be based on the third statistical query), and in case the first group of users selected by Step 908 includes the second user of Step 906 and the second estimated property of the medical data was provided to the second user, providing the third estimated property of the medical data to the first user may be withheld and/or forwent. For example, the third estimated property of the medical data may be provided in a similar fashion to the providence of the first estimated property of the medical data by Step 904 described above.

FIG. 9B illustrates an example of a method 920 for determining an estimated property of medical data. In this example, method 920 may comprise: obtaining a privacy parameter (Step 822); selecting at least one noise value based on the obtained privacy parameter (Step 824); and combining the at least one noise value with an actual property of the medical data to determine an estimated property of the medical data (Step 926). In some implementations, method 920 may comprise one or more additional steps, while some of the steps listed above may be modified or excluded. For example, in some cases Step 822 and/or

43

Step 824 and/or Step 926 may be excluded from method 920. In some implementations, one or more steps illustrated in FIG. 9B may be executed in a different order and/or one or more groups of steps may be executed simultaneously and/or a plurality of steps may be combined into single step and/or a single step may be broken down to a plurality of steps.

In some embodiments, Step 926 may comprise combining the at least one noise value selected by Step 824 with an actual property of the medical data to determine an estimated property of the medical data. For example, the actual property of the medical data may include a number, and Step 926 may manipulate the number using a noise value (for example, adding the noise value to the number, multiplying the number by the noise value, etc.) to obtain the estimated property of the medical data. In another example, the actual property of the medical data may include a list of details, and Step 926 may manipulate the list of details using the at least one noise value (for example, dropping at least part of the items in the list of details based on the at least one noise value, adding items to the list of details based on the at least one noise value, modifying items in the list of details based on the at least one noise value, switching the order of the items in the list of details based on the at least one noise value, etc.) to obtain the estimated property of the medical data.

In some embodiments, method 920 may be used one or more times. For example, method 920 may be used at a first time to determine the first estimated property of the medical data of Step 904, may be used at a second time to determine the second estimated property of the medical data of Step 912, and so forth. In some embodiments, Step 822 may obtain a first privacy parameter, Step 824 may select a first at least one noise value based on the first privacy parameter obtained by Step 822, and Step 926 may combine the first at least one noise value selected by Step 824 with a first actual property of the medical data to determine the first estimated property of the medical data of Step 904. Further, in some examples, Step 822 may obtain a second privacy parameter, Step 824 may select a second at least one noise value based on the second privacy parameter obtained by Step 822, and Step 926 may combine the second at least one noise value selected by Step 824 with a second actual property of the medical data to determine the second estimated property of the medical data of Step 912. In one example, the first privacy parameter and the second privacy parameter may be identical. In another example, the first privacy parameter may differ from the second privacy parameter. In one example, the first actual property of the medical data may be identical to the second actual property of the medical data. In another example, the first actual property of the medical data may differ from the second actual property of the medical data. In some examples, in response to the determination by Step 910 that the first group of users selected by Step 908 includes the second user of Step 906 and a first value of the first privacy parameter obtained by Step 822, the second estimated property of the medical data may be provided to the second user (for example in a similar fashion to the provision of the first estimated property of the medical data by Step 904 described above), and in response to the determination by Step 910 that the first group of users selected by Step 908 includes the second user of Step 906 and a second value of the obtained first privacy parameter, providing the second estimated property of the medical data to the second user may be withheld and/or forwent.

FIG. 9C illustrates an example of a method 930 for selectively providing information about medical data. In this

44

example, method 930 may comprise: receiving an indication that a particular change occurred to the first group of users (Step 932), for example after forgoing providing the second estimated property of the medical data to the second user by Step 914; and in response to the received indication, providing the second estimated property of the medical data to the second user (Step 934). In some implementations, method 930 may comprise one or more additional steps, while some of the steps listed above may be modified or excluded. For example, in some cases Step 932 and/or Step 934 may be excluded from method 930. In some implementations, one or more steps illustrated in FIG. 9C may be executed in a different order and/or one or more groups of steps may be executed simultaneously and/or a plurality of steps may be combined into single step and/or a single step may be broken down to a plurality of steps. In some examples, method 930 and/or Step 932 may be executed after forgoing providing the first information by Step 914 of method 900. In some examples, after completion of Step 934, method 930 may continue to execute method 940. In some examples, after completion of Step 934, method 930 may continue to execute method 960.

In some embodiments, Step 932 may comprise receiving, after Step 910 determines that the first group of users includes the second user and/or after Step 914 forgoes providing the second estimated property of the medical data to the second user, an indication that a particular change occurred to the first group of users, for example an indication that the first group of users changed to exclude a particular user, such as the first user of Step 902, the second user of Step 906, a different user, and so forth. For example, Step 932 may receive the indication from a permissions system and/or a permissions database (such as permissions 716), from a repository of regulatory statuses of users, from regulators (such as regulators 650), from a repository of user information, from a repository of employment records (for example, employment records of the user, employment records of medical care providers 630, employment records of insurers 640, employment records of regulators 650, employment records of researchers 660, employment records of facilitators 670, employment records of medical organization 110A, employment records of team 140A, etc.), and so forth. In one example, Step 932 may read the indication from memory (such as memory units 210, shared memory modules 410, and so forth). In another example, Step 932 may receive the indication from an external device over a communication network using a communication device (such as communication modules 230, internal communication modules 440, external communication modules 450, and so forth). In yet another example, Step 932 may receive the indication from a user (for example, through a user interface, through a web page, using an input device, and so forth).

In some embodiments, Step 934 may comprise providing the second estimated property of the medical data to the second user in response to an indication received by Step 932. For example, Step 934 may provide the second estimated property of the medical data to the second user in response to a first indication received by Step 932, and may withhold and/or forgo providing second estimated property of the medical data to the second user in response to a second indication received by Step 932. In another example, Step 934 may provide the second estimated property of the medical data to the second user in response to an indication received by Step 932 that the first group of users changed to exclude one user, and may withhold and/or forgo providing second estimated property of the medical data to the second

45

user in response to an indication received by Step 932 that the first group of users changed to exclude a different user. In one example, Step 934 may comprise providing the second estimated property of the medical data to the second user in response to an indication that the first group of users changed to exclude the second user received by Step 932. In another example, Step 934 may comprise providing the second estimated property of the medical data to the second user in response to an indication that the first group of users changed to exclude the first user received by Step 932.

FIG. 9D illustrates an example of a method 940 for selectively providing information about medical data. In this example, method 940 may comprise: receiving an indication that the first group of users changed to include the second user (Step 942), for example after providing the second estimated property of the medical data to the second user by Step 912 or by Step 934 or by Step 952; and in response to the received indication, providing a notification (Step 944). In some implementations, method 940 may comprise one or more additional steps, while some of the steps listed above may be modified or excluded. For example, in some cases Step 942 and/or Step 944 may be excluded from method 940. In some implementations, one or more steps illustrated in FIG. 9D may be executed in a different order and/or one or more groups of steps may be executed simultaneously and/or a plurality of steps may be combined into single step and/or a single step may be broken down to a plurality of steps. In some examples, method 940 and/or Step 942 may be executed after providing the first information by Step 912 of method 900.

In some embodiments, Step 942 may comprise receiving, after Step 910 determines that the first group of users does not include the second user and/or after Step 912 or Step 934 or Step 952 provide the second estimated property of the medical data to the second user, an indication that the first group of users changed to include the second user. For example, Step 942 may receive the indication from a permissions system and/or a permissions database (such as permissions 716), from a repository of regulatory statuses of users, from regulators (such as regulators 650), from a repository of user information, from a repository of employment records (for example, employment records of the user, employment records of medical care providers 630, employment records of insurers 640, employment records of regulators 650, employment records of researchers 660, employment records of facilitators 670, employment records of medical organization 110A, employment records of team 140A, etc.), and so forth. In one example, Step 942 may read the indication from memory (such as memory units 210, shared memory modules 410, and so forth). In another example, Step 942 may receive the indication from an external device over a communication network using a communication device (such as communication modules 230, internal communication modules 440, external communication modules 450, and so forth). In yet another example, Step 942 may receive the indication from a user (for example, through a user interface, through a web page, using an input device, and so forth).

In some embodiments, Step 944 may comprise providing a notification in response to the providence of the first estimated property of the medical data to the first user by Step 904, and/or to the providence of the second estimated property of the medical data to the second user by Step 912 or Step 934 or Step 952, and/or to the indication received by Step 942 that the first group of users changed to include the second user. In some examples, Step 944 may provide the notification to a user, to a log file, to another process, to an

46

external device, and so forth. For example, Step 944 may store the notification in memory (such as memory 700, memory units 210, memory modules 410, etc.), in storage device (such as local storage, remote storage, network attached storage, etc.), and so forth. In another example, Step 944 may transmit the notification to an external device, for example over a communication network using a communication device (such as communication modules 230, internal communication modules 440, external communication modules 450, and so forth). In some examples, Step 944 may present the notification to a user, for example through a user interface, through a web page, using an output device (such as a display screen, an augmented reality display system, a printer, a LED indicator, etc.), through computerized data analysis device 144, and so forth.

FIG. 9E illustrates an example of a method 950 for selectively providing information about medical data. In this example, method 950 may comprise: in response to the second statistical query of Step 906 belonging to a selected group of statistical queries and the determination by Step 910 that the first group of users of Step 908 includes the second user of Step 906, providing the second estimated property of the medical data to the second user (Step 952); and in response to the second statistical query of Step 906 not belonging to the selected group of statistical queries and the determination by Step 910 that the first group of users of Step 908 includes the second user of Step 906, forgoing providing the second estimated property of the medical data to the second user (Step 954). In some implementations, method 950 may comprise one or more additional steps, while some of the steps listed above may be modified or excluded. For example, in some cases Step 952 and/or Step 954 may be excluded from method 950. In some implementations, one or more steps illustrated in FIG. 9E may be executed in a different order and/or one or more groups of steps may be executed simultaneously and/or a plurality of steps may be combined into single step and/or a single step may be broken down to a plurality of steps. In some examples, method 950 may be executed after Step 910 of method 900, for example instead of Steps 914 of method 900. In some examples, after completion of Step 952, method 950 may continue to execute method 940. In some examples, after completion of Step 952, method 950 may continue to execute method 960.

In one example, the selected group of statistical queries of method 950 may include a query about a total number of patients in the medical data, may exclude a query about a number of patients that match a particular criterion, and so forth. In some examples, the selected group of statistical queries of method 950 may include a query about a statistic of a particular property in the medical data of patients in a first group of patients when the size of the first group of patients is above a selected threshold, and may exclude the query about the statistic of the particular property in the medical data of patients in the first group of patients when the size of the first group of patients is below the selected threshold. For example, the selected threshold may be based on the particular property. In another example, the selected threshold may be based on the second user of Step 906.

In some embodiments, Step 952 may comprise providing the second estimated property of the medical data of Step 912, for example to the second user of Step 906, for example in response to the second statistical query of Step 906 belonging to a selected group of statistical queries and/or to the determination by Step 910 that the first group of users of Step 908 includes the second user of Step 906.

47

In some embodiments, Step 954 may comprise forgoing providing the second estimated property of the medical data of Step 912 to the second user of Step 906 in response to the second statistical query of Step 906 not belonging to the selected group of statistical queries and/or the determination by Step 910 that the first group of users of Step 908 includes the second user of Step 906.

FIG. 9F illustrates an example of a method 960 for selectively providing information about medical data. In some examples, method 960 as well as all individual steps therein may be performed after Step 910 determined that the first group of users does not include the second user and/or after Step 912 or by Step 934 or by Step 952 provided the second estimated property of the medical data to the second user. In this example, method 960 may comprise: receiving a third statistical query about the medical data (Step 962), the third statistical query may be based on an additional input from the first user of Step 902; determining whether the first group of users selected by Step 908 changed to include the second user of Step 906 (Step 964); in response to a determination that the first group of users did not change to include the second user, providing a third estimated property of the medical data to the first user of Step 902 (Step 966), the third estimated property of the medical data may be based on the third statistical query; and in response to a determination that the first group of users changed to include the second user, forgoing providing the third estimated property of the medical data to the first user (Step 968). In some implementations, method 960 may comprise one or more additional steps, while some of the steps listed above may be modified or excluded. For example, in some cases Step 962 and/or Step 964 and/or Step 966 and/or Step 968 may be excluded from method 960. In some implementations, one or more steps illustrated in FIG. 9F may be executed in a different order and/or one or more groups of steps may be executed simultaneously and/or a plurality of steps may be combined into single step and/or a single step may be broken down to a plurality of steps.

In some embodiments, Step 962 may comprise receiving a third statistical query about the medical data, for example after Step 910 determined that the first group of users does not include the second user and/or after Step 912 or by Step 934 or by Step 952 provided the second estimated property of the medical data to the second user. For example, the third statistical query is based on an additional input from the first user. For example, Step 962 may receive the third statistical query about the medical data in a similar fashion to the reception of the first statistical query about the medical data by Step 902 described above.

In some embodiments, Step 964 may comprise determining whether the first group of users selected by Step 908 changed to include the second user of Step 906, for example after Step 910 determined that the first group of users does not include the second user and/or after Step 912 or by Step 934 or by Step 952 provided the second estimated property of the medical data to the second user. For an indication that the first group of users selected by Step 908 changed to include the second user of Step 906 may be received by Step 942 as described above, in response to such received indication, Step 964 may determine that the first group of users selected by Step 908 changed to include the second user of Step 906, and in response to a lack of such indication, Step 964 may determine that the first group of users selected by Step 908 did not change to include the second user of Step 906.

In some embodiments, Step 966 may comprise providing a third estimated property of the medical data to the first user

48

of Step 902, for example in response to a determination by Step 964 that the first group of users selected by Step 908 did not change to include the second user of Step 906. For example, the third estimated property of the medical data may be based on the third statistical query. In some examples, Step 966 may provide the third estimated property of the medical data in a similar fashion to the provision of the first estimated property of the medical data by Step 904 described above.

In some embodiments, Step 968 may comprise forgoing providing the third estimated property of the medical data of Step 966 to the first user of Step 902, for example in response to a determination by Step 964 that the first group of users selected by Step 908 changed to include the second user of Step 906.

FIG. 10 illustrates an example of a method 1000 for controlling access to private information, for example to private medical information. For example, method 1000 may control access to private information (such as private medical information) in privacy firewalls. In the example of FIG. 10, method 1000 may comprise: receiving a request to access a content of an element, the content of the element includes at least a first portion and a second portion, the first portion includes identifiable information and the second portion does not include identifiable information (Step 1002), accessing a permission record corresponding to the element (Step 1004), in response to a first value in the permission record, providing access to the content of the element, including access to the first portion and the second portion of the content of the element (Step 1006), and in response to a second value in the permission record, providing partial access to the content of the element, the partial access includes access to the second portion of the content of the element and excludes access to the first portion of the content of the element (Step 1008). In some implementations, method 1000 may comprise one or more additional steps, while some of the steps listed above may be modified or excluded. In some implementations, one or more steps illustrated in FIG. 10 may be executed in a different order and/or one or more groups of steps may be executed simultaneously and/or a plurality of steps may be combined into single step and/or a single step may be broken down to a plurality of steps.

In some examples, Step 1002 may comprise receiving a request to access a content of an element, the content of the element may include at least a first portion and a second portion, the first portion may include identifiable information and the second portion may include no identifiable information. For example, the first portion may include portion 742 or a portion of data element 750 as described above, and the second element may include portion 744 or a portion of data element 750 as described above. In one example, Step 1002 may read the request from a memory (such as memory units 210, shared memory modules 410, and so forth). In another example, Step 1002 may receive the request from an external device over a communication network using a communication device (such as communication modules 230, internal communication modules 440, external communication modules 450, and so forth). In yet another example, Step 1002 may receive the request from a user (for example, through a user interface, through a web page, using an input device, and so forth).

In some examples, receiving the request to access the content of the element by Step 1002 may comprise accessing a stream of digital communication data sent by a first computing device to a second computing device, and analyzing the stream to detect the request in the stream, for

example using a pattern matching algorithm, by parsing a protocol used for communication over the stream, and so forth. In one example, the analysis of the stream may be performed by a third computing device, the third computing device may differ from the first computing device and from the second computing device. In another example, the analysis of the stream may be performed by the second computing device. In yet another example, the analysis of the stream may be performed by the first computing device. In one example, the stream of digital communication data may be accessed by a privacy firewall, for example as described above. In another example, the stream of digital communication data may be read from a memory (such as memory units **210**, shared memory modules **410**, and so forth), may be received from an external device over a communication network using a communication device (such as communication modules **230**, internal communication modules **440**, external communication modules **450**, and so forth), may be received from a communication network using network sniffing techniques, and so forth.

In some examples, Step **1004** may comprise accessing a permission record corresponding to an element, for example corresponding to the element of Step **1002**. For example Step **1004** may access the permission record in a memory (such as memory units **210**, shared memory modules **410**, and so forth). In another example, Step **1004** may access the permission record at an external device over a communication network using a communication device (such as communication modules **230**, internal communication modules **440**, external communication modules **450**, and so forth). In yet another example, Step **1004** may access the permission record in permissions **716**.

In some examples, Step **1006** may comprise, for example in response to a first value in the permission record accessed by Step **1004**, providing access to the content of the element of Step **1002**, for example including access to the first portion and the second portion of the content of the element. In some examples, Step **1008** may comprise, for example in response to a second value in the permission record accessed by Step **1006**, providing partial access to the content of the element of Step **1002**, the partial access may include access to the second portion of the content of the element and may exclude access to the first portion of the content of the element.

In some examples, method **1000** may further comprise, for example in response to a third value in the permission record accessed by Step **1006**, providing access to synthetic information. In one example, the synthetic information may be based on the content of the element of Step **1002**. In some examples, the synthetic information may be a result of analyzing the content of the element of Step **1002** to generate the synthetic information. For example, the content of the element of Step **1002** may be analyzed to determine a distribution of values in particular portions of the element, and the determined distribution of values may be used to generate the synthetic information. In another example, the content of the element of Step **1002** may be used to train a Generative Adversarial Network (GAN), and the trained GAN may be used to generate the synthetic information.

In some examples, method **1000** may further comprise, for example in response to a third value in the permission record accessed by Step **1006**, providing statistical information based on the content of the element of Step **1002**. In some examples, the statistical information may be a result of analyzing the content of the element of Step **1002** to generate the statistical information. For example, the content of the element of Step **1002** may be analyzed to determine

a distribution of values in the element, and information may be provided based on the determined distribution of values.

In some examples, method **1000** may further comprise, for example in response to a third value in the permission record accessed by Step **1006**, providing statistical information based on a selected portion of the content of the element of Step **1002**. In some examples, the statistical information may be a result of analyzing the content of the selected portion of the content of the element Step **1002** to generate the statistical information. For example, the content of the element of Step **1002** may be analyzed to determine a distribution of values in particular portions of the element, and information may be provided based on the determined distribution of values. In one example, the selected portion of the content of the element Step **1002** may be selected based on an input from a user. In another example, the selected portion of the content of the element Step **1002** may be selected based on the content of the element Step **1002**, for example based on an analysis of the content of the element Step **1002** using an attention model trained to select portions of elements using training examples. An example of such training example may include a sample element, together with a label indicating a portion of the sample element to be selected.

In some examples, method **1000** may further comprise, for example in response to a third value in the permission record accessed by Step **1006**, denying access to the content of the element of Step **1002**.

In some examples, it may be determined whether a third portion of the content of the element of Step **1002** includes identifiable information, for example as described below. In one example, in response to a first value (for example, the first value of Step **1006**) in the permission record accessed by Step **1004**, method **1000** may provide access to the third portion of the content of the element of Step **1002**, in response to a second value in the permission record accessed by Step **1004** (for example, the second value of Step **1008**) and a determination that the third portion of the content of the element of Step **1002** includes identifiable information, method **1000** may deny access to the third portion of the content of the element of Step **1002**, and in response to a second value in the permission record accessed by Step **1004** (for example, the second value of Step **1008**) and a determination that the third portion of the content of the element of Step **1002** do not include identifiable information, method **1000** may provide access to the third portion of the content of the element of Step **1002**.

In some examples, it may be determined whether a portion of the content of the element includes identifiable information. For example, a machine learning model may be trained using training examples to determine whether portions of elements include identifiable information, and the trained machine learning model may be used to analyze the content of the element and determined whether the portion of the content of the element includes identifiable information. An example of such training example may include a sample content and an indication of a portion of the sample content, together with a label indicating whether the indicated portion of the sample content includes identifiable information. In another example, an indication of whether the portion of the content of the element includes identifiable information may be obtained (for example, from a memory, from an external device, from a user, and so forth), and the determination of whether the portion of the content of the element includes identifiable information may be based on the obtained indication. In yet another example, the determination of whether the portion of the content of the element

51

includes identifiable information may be based on type of fields included in the portion of the content of the element, may be based on a distribution of values in the portion of the content of the element, may be based on values in the portion of the content of the element, may be based on an analysis of values in the portion of the content of the element, and so forth.

In some examples, the request to access the content of the element received by Step 1002 may include an indication of a requesting entity, and the Step 1004 may further comprise selecting the permission record corresponding to the element of Step 1002 of a plurality of alternative permission records corresponding to the element of Step 1002 based on the requesting entity. For example, in response to a first requesting entity, Step 1004 may select a first permission record corresponding to the element of Step 1002, and in response to a second requesting entity, Step 1004 may select a second permission record corresponding to the element of Step 1002, the second permission record may differ from the first permission record. Some non-limiting examples of such indication of a requesting entity may include an identifier of the requesting entity (such as a name, an identification number or code, etc.), an indication of a type of the requesting entity, an identification of an organization affiliated with the requesting entity, an indication of a device used by the requesting entity for example to generate and/or to send the request (such as device name, IP address, mac address, etc.), and so forth. Some non-limiting examples of such requesting entity may include may include a person, a researcher, a physician, an organization, a division within an organization, and so forth.

In some examples, the request to access the content of the element received by Step 1002 may include an indication of an intended usage, and Step 1004 may further comprise selecting the permission record corresponding to the element of Step 1002 of a plurality of alternative permission records corresponding to the element of Step 1002 based on the intended usage. For example, in response to a first intended usage, Step 1004 may select a first permission record corresponding to the element of Step 1002, and in response to a second intended usage, Step 1004 may select a second permission record corresponding to the element of Step 1002, the second permission record may differ from the first permission record. Some non-limiting examples of such intended usage may include retrieving at least part of the content of the element, modifying at least part of the content of the element, deleting at least part of the content of the element, calculating a value of a function using at least part of the content of the element, calculating a value of a gradient of a function using at least part of the content of the element, training a machine learning model using at least part of the content of the element, generating an artificial neural network using at least part of the content of the element, generating an inference model using at least part of the content of the element, generating statistical information using at least part of the content of the element, generating synthetic data using at least part of the content of the element, and so forth. In one example, in response to an intended usage of training a first machine learning model using at least part of the content of the element, Step 1004 may select a first permission record corresponding to the element of Step 1002, and in response to an intended usage of training a second learning model using at least part of the content of the element, Step 1004 may select a second permission record corresponding to the element of Step 1002, the second permission record may differ from the first permission record. In one example, in response to an inten-

52

dent usage of calculating a value of a first function using at least part of the content of the element, Step 1004 may select a first permission record corresponding to the element of Step 1002, and in response to an intended usage of calculating a value of a second function using at least part of the content of the element, Step 1004 may select a second permission record corresponding to the element of Step 1002, the second permission record may differ from the first permission record.

In some examples, the request to access the content of the element received by Step 1002 may include and/or be a request to access the content of the element for a mathematical optimization of a function. In one example, Step 1008 may further comprise, in response to the second value in the permission record, providing access to an update information for the mathematical optimization of the function calculated using the first portion of the content of the element. For example, Step 1008 may calculate the update information for the mathematical optimization of the function using the first portion of the content of the element, and may provide the calculated update information. Some non-limiting examples of such update information may include step size, step direction, gradient, a selection of a parameter of the function to be modified, a new value for a parameter of the function, a selection of a new value of a hyperparameter of the mathematical optimization, and so forth.

In some examples, the request to access the content of the element received by Step 1002 may include and/or be a request to access the content of the element for a mathematical optimization of a function. In one example, Step 1008 may further comprise, in response to the second value in the permission record, providing access to a value of a mathematical expression of a gradient of the function calculated using the first portion of the content of the element. For example, Step 1008 may calculate the value of the mathematical expression of the gradient of the function using the first portion of the content of the element, and may provide the calculated value of the mathematical expression of the gradient of the function.

In some examples, the request to access the content of the element received by Step 1002 may include and/or be a request to access the content of the element to determine a value of a function using the first portion of the content of the element. In one example, Step 1008 may further comprise, in response to the second value in the permission record, providing access to a value of the function calculated using the first portion of the content of the element. For example, Step 1008 may calculate a value of the function using the first portion of the content of the element, and may provide the calculated value.

In some examples, an input defining a function may be received. For example, the input defining the function may be read from memory (such as memory units 210, shared memory modules 410, and so forth), may be received from external device over a communication network using a communication device (such as communication modules 230, internal communication modules 440, external communication modules 450, and so forth), may be generated, may be received from a user, and so forth. Some non-limiting examples of such function may include mathematical function, computer function, linear function, non-linear function, polynomial function, continuous function, discontinuous function, differentiable function, non-differentiable function, and so forth. In one example, Step 1008 may further comprise, in response to the second value in the permission record, causing a usage of an identified copy of the element to calculate a value of the function, and causing

53

presenting a de-identified copy of the element with the calculated value of the function. In one example, the identified copy of the element and/or the de-identified copy of the element may be obtained as described above.

In some examples, receiving the request to access the content of the element by Step 1002 may comprise accessing a stream of digital communication data sent by a first computing device to a second computing device (for example as described above), and excluding access to the first portion of the content of the element by Step 1008 may comprise accessing a second stream of digital communication data (the second stream of digital communication may be a stream sent by the second computing device to the first computing device), analyzing the second stream to detect information based on at least part of the first portion of the content of the element in the second stream, and in response to a detection of the information based on the at least part of the first portion of the content of the element, blocking at least part of the second stream from reaching the first computing device. In one example, the second stream of digital communication data may be accessed by a privacy firewall, for example as described above. In another example, the second stream of digital communication data may be read from a memory (such as memory units 210, shared memory modules 410, and so forth), may be received from an external device over a communication network using a communication device (such as communication modules 230, internal communication modules 440, external communication modules 450, and so forth), may be received from a communication network using network sniffing techniques, and so forth. In some examples, analyzing the second stream to detect information based on at least part of the first portion of the content of the element in the second stream may be performed using a pattern matching algorithm, by parsing a protocol used for communication over the stream, by using a machine learning model trained using training examples to detect information in data streams that is based on particular portions of data elements, and so forth. In some examples, in response to a detection of the information based on the at least part of the first portion of the content of the element in a particular part of the second stream, the particular part of the second stream may be blocked from reaching the first computing device, and in response to no detection of the information based on the at least part of the first portion of the content of the element in the particular part of the second stream, the particular part of the second stream may be allowed to reach the first computing device.

In some examples, receiving the request to access the content of the element by Step 1002 may comprise accessing a stream of digital communication data sent by a first computing device to a second computing device (for example as described above), and excluding access to the first portion of the content of the element by Step 1008 may comprise modifying at least part of the stream of digital communication data to obtain a modified stream, and providing the modified stream to the second computing device. For example, the at least part of the stream of digital communication data may be modified to omit or to modify the request to access the content of the element of Step 1002.

In some examples, receiving the request to access the content of the element by Step 1002 may comprise accessing a stream of digital communication data sent by a first computing device to a second computing device (for example as described above), step 1006 may comprise, in response to the first value in the permission record, allowing at least part of the stream of digital communication data to

54

reach the second computing device, and method 1000 may further comprise in response to a third value in the permission record, blocking the at least part of the stream of digital communication data from reaching the second computing device. For example, the third value may be identical to the second value of Step 1008, may differ from the second value of Step 1008, may differ from the first value of Step 1006, and so forth.

FIG. 11 illustrates an example of a method 1100 for ownership determination, for example for ownership determination in privacy firewalls. In this example, method 1100 may comprise: receiving a request of a user to perform an action for creating a new data collection using one or more source data collections (Step 1102), accessing one or more ownership records to determine ownership status of the one or more source data collections (Step 1104), accessing one or more permission records to determine permission status of the user in relation to the one or more source data collections (Step 1106), in response to a determination that the user does not have permission to view at least part of at least one of the one or more source data collections and that the user is not an owner of the at least one of the one or more source data collections, determining that the user is not an owner of the new data collection (Step 1108), and in response to a determination that for each data collection of the one or more source data collections the user is at least one of an owner of the data collection or has permission to view the entire data collection, determining that the user is an owner of the new data collection (Step 1110). In some implementations, method 1100 may comprise one or more additional steps, while some of the steps listed above may be modified or excluded. In some implementations, one or more steps illustrated in FIG. 11 may be executed in a different order and/or one or more groups of steps may be executed simultaneously and/or a plurality of steps may be combined into single step and/or a single step may be broken down to a plurality of steps.

In some examples, method 1100 may further comprise performing the action (of Step 1102) for creating the new data collection using the one or more source data collections. In some examples, the action (of Step 1102) for creating the new data collection using the one or more source data collections may comprise selecting a parameter for optimizing a function of data included in the one or more source data collections, and in one example, the new data collection may include at least one value of the optimized function. Some non-limiting examples of such parameters may include a hyper-parameter (for example, of an artificial neural network, of a machine learning algorithm, of a kernel function, of a family of functions, etc.), a power and/or a base of an exponent expression, a numerator, a denominator, and so forth. In some examples, the action (of Step 1102) for creating the new data collection using the one or more source data collections may comprise calculating a value of a function of data included in the one or more source data collections, and in one example, the new data collection may include the calculated value of the function of the data. Some non-limiting examples of such function may include a classification function, a regression function, a function learnt using a machine learning model, an artificial neural network, a polynomial function, an exponential function, a linear function, a non-linear function, and so forth. In some examples, the action (of Step 1102) for creating the new data collection using the one or more source data collections may comprise calculating a gradient of a function of data included in the one or more source data collections. Some non-limiting examples of such function may include a

55

classification function, a regression function, an intermediate function in an optimization and/or a machine learning algorithm learning process, a function learnt using a machine learning model, an artificial neural network, a polynomial function, an exponential function, a linear function, a non-linear function, and so forth. In one example, the new data collection may include the calculated gradient of the function of data. In another example, the new data collection may be based on the calculated gradient of the function of data. For example, in response to a first calculated gradient of the function of data, a first new data collection may be generated, and in response to a second calculated gradient of the function of data, a second new data collection may be generated, the second new data collection may differ from the first new data collection. In some examples, the action (of Step 1102) for creating the new data collection using the one or more source data collections may comprise calculating a statistical measurement of data included in the one or more source data collections, and in one example, the new data collection may include the calculated statistical measurement. Some non-limiting examples of such statistical measurement may include mean, median, mode, variance, standard deviation, histogram, entropy, and so forth. In some examples, method 1100 may further comprise, for example in response to a determination by Step 1106 that the user does not have permission to use at least part of the one or more source data collections to create different data collections, denying the request received by Step 1102.

In some examples, method 1100 may further comprise updating the one or more ownership records accessed by Step 1104 based on the determination of whether the user is an owner of the new data collection. For example, in response to a determination that the user is an owner of the new data collection, method 1100 may make a first update to the one or more ownership records accessed by Step 1104, and in response to a determination that the user is not an owner of the new data collection, method 1100 may make a second update to the one or more ownership records accessed by Step 1104, the second update may differ from the first update. In another example, in response to a determination that the user is an owner of the new data collection, method 1100 may make a first update to the one or more ownership records accessed by Step 1104, and in response to a determination that the user is not an owner of the new data collection, method 1100 may forgo making the first update to the one or more ownership records accessed by Step 1104.

In some examples, method 1100 may further comprise updating the one or more permission records accessed by Step 1106 based on the determination of whether the user is an owner of the new data collection determined using Step 1104 and/or based on the permission status of the user in relation to the one or more source data collections determined by Step 1106. For example, in response to a determination that the user is an owner of the new data collection, method 1100 may make a first update to the one or more permission records accessed by Step 1106, and in response to a determination that the user is not an owner of the new data collection, method 1100 may make a second update to the one or more permission records accessed by Step 1106, the second update may differ from the first update. In another example, in response to a determination that the user is an owner of the new data collection, method 1100 may make a first update to the one or more permission records accessed by Step 1106, and in response to a determination that the user is not an owner of the new data collection,

56

method 1100 may forgo making the first update to the one or more permission records accessed by Step 1106. In yet another example, in response to a first permission status of the user in relation to the one or more source data collections, method 1100 may make a first update to the one or more permission records accessed by Step 1106, and in response to a second permission status of the user in relation to the one or more source data collections, method 1100 may make a second update to the one or more permission records accessed by Step 1106, the second update may differ from the first update. In an additional example, in response to a first permission status of the user in relation to the one or more source data collections, method 1100 may make a first update to the one or more permission records accessed by Step 1106, and in response to a second permission status of the user in relation to the one or more source data collections, method 1100 may forgo making the first update to the one or more permission records accessed by Step 1106. In yet another example, in response to a first combination of ownership status determined by Step 1104 and permission status determined by Step 1106, method 1100 may make a first update to the one or more permission records accessed by Step 1106, and in response to a second combination of ownership status determined by Step 1104 and permission status determined by Step 1106, method 1100 may make a second update to the one or more permission records accessed by Step 1106, the second update may differ from the first update. In an additional example, in response to a first combination of ownership status determined by Step 1104 and permission status determined by Step 1106, method 1100 may make a first update to the one or more permission records accessed by Step 1106, and in response to a second combination of ownership status determined by Step 1104 and permission status determined by Step 1106, method 1100 may forgo making the first update to the one or more permission records accessed by Step 1106.

In some examples, the one or more source data collections of Step 1102 may include a plurality of records, the action (of Step 1102) for creating the new data collection using the one or more source data collections may comprise training a machine learning model using a first portion of the plurality of records, and the new data collection of Step 1102 may include at least a prediction of the trained machine learning model for at least one record of the plurality of records not included in the first portion of the plurality of records.

In some examples, Step 1102 may comprise receiving a request of a user to perform an action for creating a new data collection using one or more source data collections. In one example, Step 1102 may read the request from a memory (such as memory units 210, shared memory modules 410, and so forth). In another example, Step 1102 may receive the request from an external device over a communication network using a communication device (such as communication modules 230, internal communication modules 440, external communication modules 450, and so forth). In yet another example, Step 1102 may receive the request from the user (for example, through a user interface, through a web page, using an input device, and so forth).

In some examples, receiving the request of the user by Step 1102 may comprise accessing a stream of digital communication data sent by a first computing device to a second computing device, and analyzing the stream to detect the request in the stream, for example using a pattern matching algorithm, by parsing a protocol used for communication over the stream, and so forth. In one example, the analysis of the stream may be performed by a third com-

57

puting device, the third computing device may differ from the first computing device and from the second computing device. In another example, the analysis of the stream may be performed by the second computing device. In yet another example, the analysis of the stream may be performed by the first computing device. In one example, the second computing device may be configured to perform the action for creating the new data collection using the one or more source data collections in response to the request of the user. In one example, the stream of digital communication data may be accessed by a privacy firewall, for example as described above. In another example, the stream of digital communication data may be read from a memory (such as memory units 210, shared memory modules 410, and so forth), may be received from an external device over a communication network using a communication device (such as communication modules 230, internal communication modules 440, external communication modules 450, and so forth), may be received from a communication network using network sniffing techniques, and so forth.

In some examples, Step 1104 may comprise accessing one or more ownership records to determine ownership status of the one or more source data collections of Step 1102. For example Step 1104 may access the one or more ownership records in a memory (such as memory units 210, shared memory modules 410, and so forth). In another example, Step 1104 may access the one or more ownership records at an external device over a communication network using a communication device (such as communication modules 230, internal communication modules 440, external communication modules 450, and so forth). For example, the ownership records may include an identifier of an owner of a source data collection for at least some of the one or more source data collections, may include type of ownership corresponding to a source data collection for at least some of the one or more source data collections, and so forth. Some non-limiting examples of such type of ownership may include 'full ownership', 'conditional ownership', 'sole ownership', 'joint ownership', 'ownership due to creation', 'ownership due to assignment', and so forth. In some examples, the ownership status may include at least one of the identities of the owners, the type of the ownership, a category indicative of the owners, and so forth.

In some examples, Step 1106 may comprise accessing one or more permission records to determine permission status of the user of Step 1102 in relation to the one or more source data collections of Step 1102. For example Step 1106 may access the one or more permission records in a memory (such as memory units 210, shared memory modules 410, and so forth). In another example, Step 1106 may access the one or more permission records at an external device over a communication network using a communication device (such as communication modules 230, internal communication modules 440, external communication modules 450, and so forth). In yet another example, Step 1106 may access the one or more permission records in permissions 716. For example, the permission records may include an indication of a permission corresponding to a user (or a group of users that including the user) and a source data collection for at least some of the one or more source data collections. Other examples are described above, for example with relation to permissions 716. In some examples, the permission status may include at least one of a permission corresponding to the user of Step 1102 and at least one of the one or more source data collections of Step 1102 (such as 'read only', 'edit', etc.), a type of the permission (such as 'temporary', 'permanent', etc.), and so forth.

58

In some examples, Step 1108 may comprise, for example in response to a determination by Step 1106 that the user of Step 1102 does not have permission to view at least part of at least one of the one or more source data collections of Step 1102 and to a determination by Step 1104 that the user of Step 1102 is not an owner of the at least one of the one or more source data collections of Step 1102, determining that the user of Step 1102 is not an owner of the new data collection of Step 1102.

In some examples, Step 1110 may comprise, for example in response to a determination by Step 1104 and/or Step 1106 that for each data collection of the one or more source data collections of Step 1102 the user of Step 1102 is at least one of an owner of the data collection or has permission to view the entire data collection, determining that the user of Step 1102 is an owner of the new data collection.

In some examples, method 1100 may further comprise determining at least one owner of the new data collection, for example based on the ownership status of the one or more source data collections determined by Step 1104 and/or based on the permission status of the user in relation to the one or more source data collections determined by Step 1106. The determined at least one owner may include the user, may not include the user, may include the user and at least one additional entity, may be the user, may be a single owner, may be a plurality of owners, and so forth. For example, in response to a first ownership status, method 1100 may determining a first at least one owner of the new data collection, and in response to a second ownership status, method 1100 may determining a second at least one owner of the new data collection, the second at least one owner of the new data collection may differ from the first at least one owner of the new data collection. In another example, in response to a first combination of ownership status and permission status, method 1100 may determining a first at least one owner of the new data collection, and in response to a second combination of ownership status and permission status, method 1100 may determining a second at least one owner of the new data collection, the second at least one owner of the new data collection may differ from the first at least one owner of the new data collection. In yet another example, in response to a first permission status, method 1100 may determining a first at least one owner of the new data collection, and in response to a second permission status, method 1100 may determining a second at least one owner of the new data collection, the second at least one owner of the new data collection may differ from the first at least one owner of the new data collection.

In some examples, method 1100 may further comprise determining a size of the new data collection. Some non-limiting examples of such size of data collection may include storage size of the data collection (for example in bytes, bits, etc.), number of data-points in the data collection, entropy of the data collection, mathematical cardinality of the data collection, mathematical dimension of the data collection, Vapnik-Chervonenkis dimension related to the data collection, and so forth. Further, in some examples, in response to a first size of the new data collection, method 1100 may determine a first permission of the user in relation to the new data collection, and in response to a second size of the new data collection, method 1100 may determine a second permission of the user in relation to the new data collection, the second permission may differ from the first permission. Some non-limiting examples of such examples may include permission to modify the new data collection, permission to delete the new data collection, permission to read data from the new data collection, permission to obtain

59

statistical measurements of the new data collection, permission to obtain synthetic data generated based on the new data collection, and so forth.

FIG. 12 illustrates an example of a method 1200 for determining permissions, for example for determining permissions in privacy firewalls. In this example, method 1200 may comprise: analyzing at least part of a content of a data collection to determine a subject matter (Step 1202), determining a permission corresponding to the data collection and at least one user based on the subject matter (Step 1204), receiving a request of the at least one user to access at least part of the data collection (Step 1206), in response to a first determined permission, providing the requested access to the at least part of the data collection (Step 1208), and in response to a second determined permission, denying the request (Step 1210). In some implementations, method 1200 may comprise one or more additional steps, while some of the steps listed above may be modified or excluded. In some implementations, one or more steps illustrated in FIG. 12 may be executed in a different order and/or one or more groups of steps may be executed simultaneously and/or a plurality of steps may be combined into single step and/or a single step may be broken down to a plurality of steps.

In some examples, Step 1202 may comprise analyzing at least part of a content of a data collection to determine a subject matter. For example, a machine learning model may be trained using training examples to determine subject matter from content (for example, of data collections), and Step 1202 may use the trained machine learning model to analyze the at least part of a content of a data collection and determine the subject matter. An example of such training example may include a sample content, together with a label indicating the subject matter. In another example, the at least part of a content of a data collection may include textual information, and Natural Language Processing algorithms (such as topic identification algorithms) may be used to analyze the textual information and determine the subject. In yet another example, the at least part of a content of a data collection may include visual information, and computer vision algorithms may be used to analyze the visual information to determine the subject of the visual information. In an additional example, a classification algorithm may be used to classify the at least part of a content of a data collection to one of a plurality of alternative subject matters.

In some examples, the at least part of the content of the data collection of Step 1202 may include at least one or more medical images, and Step 1202 may comprise analyzing the one or more medical images to determine the subject matter. In one example, a convolution of a plurality of pixels of the one or more medical images may be calculated, and Step 1202 may use the calculated convolution to determine the subject matter. For example, in response to a first value of the calculated convolution, Step 1202 may determine that a first subject matter corresponds to the data collection, and in response to a second value of the calculated convolution, Step 1202 may determine that a second subject matter corresponds to the data collection, the second subject matter may differ from the first subject matter. In one example, one or more pixels of at least one of the one or more medical images may be analyzed to generate a transformed image, and Step 1202 may use the transformed image to determine the subject matter. For example, in response to a first transformed image, Step 1202 may determine that a first subject matter corresponds to the data collection, and in response to a second transformed image, Step 1202 may

60

determine that a second subject matter corresponds to the data collection, the second subject matter may differ from the first subject matter.

In some examples, the at least part of the content of the data collection of Step 1202 may include at least textual information, and Step 1202 may comprise analyzing the textual information to determine the subject matter. For example, in response to a first textual information, Step 1202 may determine that a first subject matter corresponds to the data collection, and in response to a second textual information, Step 1202 may determine that a second subject matter corresponds to the data collection, the second subject matter may differ from the first subject matter. In one example, the textual information may be analyzed to determine word prevalence of at least one word in at least a portion of the textual information, and Step 1202 may use the determined word prevalence to determine the subject matter. For example, in response to a first word prevalence, Step 1202 may determine that a first subject matter corresponds to the data collection, and in response to a second word prevalence, Step 1202 may determine that a second subject matter corresponds to the data collection, the second subject matter may differ from the first subject matter.

In some examples, the at least part of the content of the data collection of Step 1202 may include at least one or more audio recordings, and Step 1202 may comprise analyzing the one or more audio recordings to determine the subject matter, for example using one or more audio analysis algorithms. For example, in response to a first audio recording, Step 1202 may determine that a first subject matter corresponds to the data collection, and in response to a second audio recording, Step 1202 may determine that a second subject matter corresponds to the data collection, the second subject matter may differ from the first subject matter. In one example, a convolution of at least part of the one or more audio recordings may be calculated, and Step 1202 may use the calculated convolution to determine the subject matter. For example, in response to a first value of the calculated convolution, Step 1202 may determine that a first subject matter corresponds to the data collection, and in response to a second value of the calculated convolution, Step 1202 may determine that a second subject matter corresponds to the data collection, the second subject matter may differ from the first subject matter.

In some examples, Step 1204 may comprise determining a permission corresponding to the data collection of Step 1202 and at least one user based on the subject matter determined by Step 1202. Some non-limiting examples of such permission may include permission for the at least one user to modify the data collection, permission for the at least one user to delete the data collection, permission for the at least one user to read data from the data collection, permission for the at least one user to obtain statistical measurements of the data collection, permission for the at least one user to obtain synthetic data generated based on the data collection, and so forth. For example, in response to a first subject matter determined by Step 1202, Step 1204 may determine a first permission corresponding to the data collection and the at least one user, and in response to a second subject matter determined by Step 1202, Step 1204 may determine a second permission corresponding to the data collection and the at least one user, the second permission may differ from the first permission.

In some examples, the subject matter may correspond to a body organ, in response to a first body organ corresponding to the subject matter, Step 1204 may determine a first permission corresponding to the data collection and the at

61

least one user, and in response to a second body organ corresponding to the subject matter, Step 1204 may determine a second permission corresponding to the data collection and the at least one user, the second permission may differ from the first permission. In some examples, the subject matter may correspond to a medical specialty, in response to a first medical specialty corresponding to the subject matter, Step 1204 may determine a first permission corresponding to the data collection and the at least one user, and in response to a second medical specialty corresponding to the subject matter, Step 1204 may determine a second permission corresponding to the data collection and the at least one user, the second permission may differ from the first permission. In some examples, the subject matter may correspond to a disease, in response to a first disease corresponding to the subject matter, Step 1204 may determine a first permission corresponding to the data collection and the at least one user, and in response to a second disease corresponding to the subject matter, Step 1204 may determine a second permission corresponding to the data collection and the at least one user, the second permission may differ from the first permission. In some examples, the subject matter may correspond to a medical condition, in response to a first medical condition corresponding to the subject matter, Step 1204 may determine a first permission corresponding to the data collection and the at least one user, and in response to a second medical condition corresponding to the subject matter, Step 1204 may determine a second permission corresponding to the data collection and the at least one user, the second permission may differ from the first permission.

In some examples, Step 1204 may determine the permission corresponding to the data collection of Step 1202 and the at least one user based on the subject matter and a property of the at least one user. For example, in response to a first combination of subject matter and property of the at least one user, Step 1204 may determine a first permission corresponding to the data collection and the at least one user, and in response to a second combination of subject matter and property of the at least one user, Step 1204 may determine a second permission corresponding to the data collection and the at least one user, the second permission may differ from the first permission. Some non-limiting examples of such property of the at least one user may include an affiliation of the at least one user, a medical specialty corresponding to the at least one user, an demographic detail of the at least one user, a geographic location corresponding to the at least one user, payment data corresponding to the at least one user, privileges of the at least one user, past behavior of the at least one user, and so forth. For example, the property of the at least one user may be an affiliation of the at least one user, in response to a first combination of subject matter and affiliation of the at least one user, Step 1204 may determine a first permission corresponding to the data collection and the at least one user, and in response to a second combination of subject matter and affiliation of the at least one user, Step 1204 may determine a second permission corresponding to the data collection and the at least one user, the second permission may differ from the first permission. In another example, the property of the at least one user may be a medical specialty corresponding to the at least one user, in response to a first combination of subject matter and medical specialty corresponding to the at least one user, Step 1204 may determine a first permission corresponding to the data collection and the at least one user, and in response to a second combination of subject matter and medical specialty corresponding

62

to the at least one user, Step 1204 may determine a second permission corresponding to the data collection and the at least one user, the second permission may differ from the first permission.

In some examples, Step 1206 may comprise receiving a request of the at least one user of Step 1204 to access at least part of the data collection of Step 1202. In one example, Step 1206 may read the request from a memory (such as memory units 210, shared memory modules 410, and so forth). In another example, Step 1206 may receive the request from an external device over a communication network using a communication device (such as communication modules 230, internal communication modules 440, external communication modules 450, and so forth). In yet another example, Step 1206 may receive the request from a user (for example, through a user interface, through a web page, using an input device, and so forth).

In some examples, receiving the request of the user by Step 1206 may comprise accessing a stream of digital communication data sent by a first computing device to a second computing device, and analyzing the stream to detect the request in the stream, for example using a pattern matching algorithm, by parsing a protocol used for communication over the stream, and so forth. In one example, the analysis of the stream may be performed by a third computing device, the third computing device may differ from the first computing device and from the second computing device. In another example, the analysis of the stream may be performed by the second computing device. In yet another example, the analysis of the stream may be performed by the first computing device. In one example, the second computing device may be configured to access the at least part of the data collection in response to the request of the user. In one example, the stream of digital communication data may be accessed by a privacy firewall, for example as described above. In another example, the stream of digital communication data may be read from a memory (such as memory units 210, shared memory modules 410, and so forth), may be received from an external device over a communication network using a communication device (such as communication modules 230, internal communication modules 440, external communication modules 450, and so forth), may be received from a communication network using network sniffing techniques, and so forth.

In some examples, Step 1208 may comprise, for example in response to a first determined permission, providing the requested access to the at least part of the data collection. In some examples, Step 1210 may comprise, for example in response to a second determined permission, denying the request received by Step 1206 to access the at least part of the data collection. In some examples, the data collection of Step 1202 may include a first portion and a second portion, the first portion may include identifiable information and the second portion may include no identifiable information, in response to a third determined permission, method 1200 may provide access to the content of the data collection, including access to the first portion and the second portion of the data collection, and in response to a fourth determined permission, method 1200 may provide partial access to the data collection, the partial access may include access to the second portion of the data collection and may exclude access to the first portion of the data collection.

In some examples, method 1200 may further comprise, for example in response to a third determined permission, providing access to synthetic information based on the data collection of Step 1202. In some examples, the synthetic information may be a result of analyzing the content of the

63

data collection of Step 1202 to generate the synthetic information. For example, the content of the data collection of Step 1202 may be analyzed to determine a distribution of values in particular portions of the data collection, and the determined distribution of values may be used to generate the synthetic information. In another example, the content of the data collection of Step 1202 may be used to train a Generative Adversarial Network (GAN), and the trained GAN may be used to generate the synthetic information.

In some examples, method 1200 may further comprise, for example in response to a third determined permission, providing access to statistical information based on the data collection. In some examples, the statistical information may be a result of analyzing content of the data collection of Step 1202 or of a portion of the data collection of Step 1202 to generate the statistical information. For example, the content of the data collection of Step 1202 or of the portion of the data collection of Step 1202 may be analyzed to determine a distribution of values in the data collection or in the portion of the data collection of Step 1202, and information may be provided based on the determined distribution of values.

In some examples, receiving the request of the user by Step 1206 may comprise accessing a stream of digital communication data sent by a first computing device to a second computing device (for example as described above), and denying the request by Step 1210 may comprise accessing a second stream of digital communication data (the second stream of digital communication may be a stream sent by the second computing device to the first computing device), analyzing the second stream to detect information based on the at least part of the data collection, and in response to a detection of the information based on the at least part of the data collection, blocking at least part of the second stream from reaching the first computing device. In one example, the second stream of digital communication data may be accessed by a privacy firewall, for example as described above. In another example, the second stream of digital communication data may be read from a memory (such as memory units 210, shared memory modules 410, and so forth), may be received from an external device over a communication network using a communication device (such as communication modules 230, internal communication modules 440, external communication modules 450, and so forth), may be received from a communication network using network sniffing techniques, and so forth. In some examples, analyzing the second stream to detect information based on the at least part of the data collection in the second stream may be performed using a pattern matching algorithm, by parsing a protocol used for communication over the stream, by using a machine learning model trained using training examples to detect information in data streams that is based on particular portions of data elements, and so forth. In some examples, in response to a detection of the information based on the at least part of the data collection in a particular part of the second stream, the particular part of the second stream may be blocked from reaching the first computing device, and in response to no detection of the information based on the at least part of the data collection in the particular part of the second stream, the particular part of the second stream may be allowed to reach the first computing device.

In some examples, receiving the request of the user by Step 1206 may comprise accessing a stream of digital communication data sent by a first computing device to a second computing device (for example as described above), and denying the request by Step 1210 may comprise modifying at least part of the stream of digital communication

64

data to obtain a modified stream, and providing the modified stream to the second computing device. For example, the at least part of the stream of digital communication data may be modified to omit or to modify the request to access the at least part of the data collection of Step 1206.

In some examples, receiving the request of the user by Step 1206 may comprise accessing a stream of digital communication data sent by a first computing device to a second computing device (for example as described above), and step 1208 may comprise, in response to the first determined permission, allowing at least part of the stream of digital communication data to reach the second computing device, and method 1200 may further comprise in response to a third determined permission, blocking the at least part of the stream of digital communication data from reaching the second computing device. For example, the third determined permission may be identical to the second determined permission of Step 1210, may differ from the second determined permission of Step 1210, may differ from the first determined permission of Step 1208, and so forth.

FIG. 13 illustrates an example of a method 1300 for detecting identified information, for example for detecting identified information in privacy firewalls. In this example, method 1300 may comprise: accessing a data collection to identify a repeating field in the data collection (Step 1302), analyzing content of the field in the data collection to determine whether the field is likely to include information that identifies at least one particular individual (Step 1304), receiving an access request of a user (Step 1306), accessing a permission record associated with the user (Step 1308), in response to a determination that the field is likely to include information that identifies at least one particular individual and a first value in the permission record, denying access of the user to at least part of the content of the field in the data collection (Step 1310), in response to a determination that the field is not likely to include information that identifies at least one particular individual and the first value in the permission record, providing access of the user to the at least part of the content of the field in the data collection (Step 1312), and in response to a second value in the permission record, providing access of the user to the at least part of the content of the field in the data collection (Step 1314). In some implementations, method 1300 may comprise one or more additional steps, while some of the steps listed above may be modified or excluded. In some implementations, one or more steps illustrated in FIG. 13 may be executed in a different order and/or one or more groups of steps may be executed simultaneously and/or a plurality of steps may be combined into single step and/or a single step may be broken down to a plurality of steps.

In some examples, Step 1302 may comprise accessing a data collection to identify a repeating field in the data collection. Some non-limiting examples of such repeating field may include a row or a column in a data table comprising a plurality of values corresponding to the same field, a field in a data structure where the data collection includes a plurality of instances of the data structure and therefore a plurality of values of the field, a field in a form where the data collection includes a plurality of copies of the form and therefore a plurality of values of the field, and so forth. In some non-limiting examples, the repeating field in the data collection may include data of patients, identifiers of patients, names of patients, phone numbers of patients, address of patients, demographic information of patients, data of physicians, identifiers of physicians, names of physicians, data of appointments, time of appointments, participants of appointments, types of appointments, data of medi-

65

cations, name of medication, dosages of medications, data of prescriptions, date of prescriptions, medications in prescriptions, data of offices, data of surgeries, data of medical devices, data of medical tests, and so forth.

In some examples, Step 1304 may comprise analyzing content of a field, such as the field identified as a repeating field in the data collection by Step 1302, to determine whether the field is likely to include information that identifies at least one particular individual. For example, Step 1304 may base the determination of whether the field is likely to include information that identifies at least one particular individual on one or more of a type of the field, a distribution of values in the field, values in the field, analysis of values in the field, other fields, types of other fields, distributions of values in other fields, values in other fields, analysis of values in other fields, and so forth. In some examples, Step 1304 may comprise analyzing the content of the field in the data collection identified by Step 1302 as a repeated field using a machine learning model to determine whether the field is likely to include information that identifies at least one particular individual. For example, a machine learning model may be trained using training examples to determine whether fields are likely to include information that identifies individuals or particular type of individuals from the content of the fields, and Step 1304 may use the trained machine learning model to analyze the content of the field and determine whether the field is likely to include information that identifies at least one particular individual. An example of such training example may include a sample content of a sample field together with a label indicating whether the sample field include information that identifies at least one particular individual.

In some examples, Step 1304 may comprise searching for keywords in the content of the field in the data collection identified by Step 1302 as a repeated field to determine whether the field is likely to include information that identifies at least one particular individual. For example, in response to a detection of a particular keyword in the content of the field, Step 1304 may determine that the field is likely to include information that identifies at least one particular individual, and in response to no detection of the particular keyword in the content of the field, Step 1304 may determine that the field is not likely to include information that identifies at least one particular individual. In another example, in response to a detection of a particular keyword in the content of the field, Step 1304 may determine that the field is not likely to include information that identifies at least one particular individual, and in response to no detection of the particular keyword in the content of the field, Step 1304 may determine that the field is likely to include information that identifies at least one particular individual. In yet another example, in response to a detection of a particular combination of keywords in the content of the field, Step 1304 may determine that the field is likely to include information that identifies at least one particular individual, and in response to no detection of the particular combination of keywords in the content of the field, Step 1304 may determine that the field is not likely to include information that identifies at least one particular individual. In some examples, Step 1304 may comprise analyzing a distribution of values in the content of the field in the data collection identified by Step 1302 as a repeated field to determine whether the field is likely to include information that identifies at least one particular individual. For example, in response to a first distribution of values in the content of the field, Step 1304 may determine that the field is likely to include information that identifies at least one particular

66

individual, and in response to a second distribution of values in the content of the field, Step 1304 may determine that the field is not likely to include information that identifies at least one particular individual. In some examples, Step 1304 may comprise analyzing content of a second field in the data collection of Step 1302 (for example, different than the field in the data collection identified by Step 1302 as a repeated field) to determine whether the field in the data collection identified by Step 1302 as a repeated field is likely to include information that identifies at least one particular individual. For example, in response to a first content of the second field, Step 1304 may determine that the field is likely to include information that identifies at least one particular individual, and in response to a second content of the second field, Step 1304 may determine that the field is not likely to include information that identifies at least one particular individual.

In some examples, the content of the field in the data collection identified by Step 1302 as a repeated field may include one or more audio recordings, and Step 1304 may analyze content of at least part of the one or more audio recordings to determine whether the field is likely to include information that identifies at least one particular individual. For example, Step 1304 may use a speech detection algorithm to determine whether the at least part of the one or more audio recordings includes a voice of a person, in response to a determination that the at least part of the one or more audio recordings includes a voice of a person, Step 1304 may determine that the field is likely to include information that identifies at least one particular individual, and in response to a determination that the at least part of the one or more audio recordings does not include a voice of a person, Step 1304 may determine that the field is not likely to include information that identifies at least one particular individual. In another example, Step 1304 may use speech to text algorithms to obtain textual information corresponding to speech in the at least part of the one or more audio recordings, and Step 1304 may analyze the obtained textual information, for example as described below, to determine whether the field is likely to include information that identifies at least one particular individual.

In some examples, the content of the field in the data collection identified by Step 1302 as a repeated field may include textual information, and Step 1304 may analyze content of at least part of the textual information to determine whether the field is likely to include information that identifies at least one particular individual. For example, keywords may be searched in the at least part of the textual information to determine whether the field is likely to include information that identifies at least one particular individual, for example as described above. In another example, Step 1304 may use Natural Language Processing (NLP) algorithms to analyze the at least part of the textual information and determine whether the field is likely to include information that identifies at least one particular individual. In yet another example, a machine learning classification model may be trained using training examples to determine whether textual data includes identifying information of individuals, and Step 1304 may use the trained machine learning classification model to analyze the at least part of the textual information and determine whether the field is likely to include information that identifies at least one particular individual. An example of such training example may include a sample textual information together with a label indicating whether the sample textual information includes information that identifies at least one particular individual.

67

In some examples, the content of the field in the data collection identified by Step 1302 as a repeated field includes numerical data, and Step 1304 may analyze content of at least part of the numerical data to determine whether the field is likely to include information that identifies at least one particular individual. For example, a machine learning classification model may be trained using training examples to determine whether numerical data includes identifying information of individuals, and Step 1304 may use the trained machine learning classification model to analyze the at least part of the numerical data and determine whether the field is likely to include information that identifies at least one particular individual. An example of such training example may include a sample numerical data together with a label indicating whether the sample numerical data includes information that identifies at least one particular individual. In another example, distribution of values of the numerical data may be determined, in response to a first determined distribution, Step 1304 may determine that the field is likely to include information that identifies at least one particular individual, and in response to a second determined distribution, Step 1304 may determine that the field is not likely to include information that identifies at least one particular individual.

In some examples, the content of the field in the data collection identified by Step 1302 as a repeated field may include one or more images, and Step 1304 may analyze the visual content of at least part of the one or more images to determine whether the field is likely to include information that identifies at least one particular individual. For example, an OCR algorithm may be used to extract textual information from the at least part of the one or more images, and Step 1304 may analyze the extracted textual information (for example as described above) to determine whether the field is likely to include information that identifies at least one particular individual. In another example, face detection algorithms may be used to detect faces depicted in the at least part of the one or more images, in response to a detection of a face in the at least part of the one or more images, Step 1304 may determine that the field is likely to include information that identifies at least one particular individual, and in response to no detection of faces in the at least part of the one or more images, Step 1304 may determine that the field is not likely to include information that identifies at least one particular individual. In yet another example, face recognition algorithms may be used to recognize individuals depicted in the at least part of the one or more images, in response to a recognition of particular individuals in the at least part of the one or more images, Step 1304 may determine that the field is likely to include information that identifies at least one particular individual, and in response to no recognition of the particular individuals in the at least part of the one or more images, Step 1304 may determine that the field is not likely to include information that identifies at least one particular individual. In one example, Step 1304 may analyze the visual content of the at least part of the one or more images to determine whether the at least part of the one or more images includes a depiction of a text (for example using text detection algorithms), in response to a determination that the at least part of the one or more images includes a depiction of a text, Step 1304 may determine that the field is likely to include information that identifies at least one particular individual, and in response to a determination that the at least part of the one or more images does not include a depiction of a text, Step 1304 may determine that the field is not likely to include information that identifies at least one particular

68

individual. In one example, Step 1304 may analyze the visual content of the at least part of the one or more images to determine whether the at least part of the one or more images includes a depiction of a face (for example using face detection algorithms), in response to a determination that the at least part of the one or more images includes a depiction of a face, Step 1304 may determine that the field is likely to include information that identifies at least one particular individual, and in response to a determination that the at least part of the one or more images does not include a depiction of a face, Step 1304 may determine that the field is not likely to include information that identifies at least one particular individual. In one example, Step 1304 may analyze the visual content of the at least part of the one or more images to determine whether the at least part of the one or more images includes a depiction of a skin mark, and may analyze the depiction of the skin mark to determine whether the field is likely to include information that identifies at least one particular individual. Some non-limiting examples of such skin marks may include one or more of scars, tattoos, birth marks, and so forth. For example, a visual detector may be trained using training examples to detect skin marks in images, and Step 1304 may use the trained visual detector to analyze the visual content of the at least part of the one or more images to determine whether the at least part of the one or more images includes a depiction of a skin mark. An example of such training example may include a sample image together with a label indicating whether the sample image includes a skin mark and/or the location of the skin mark in the sample image. For example, a machine learning classifier may be trained using training examples to determine whether skin marks identifies at least one particular individual, and Step 1304 may use the trained machine learning classifier to analyze the depiction of the skin mark to determine whether the field is likely to include information that identifies at least one particular individual. An example of such training example may include a sample image of a skin mark, together with a label indicating whether the skin mark depicted in the sample image identifies at least one particular individual. In some examples, Step 1304 may calculate a convolution of a plurality of pixels of the at least part of the one or more images, and may use the calculated convolution to determine whether the field is likely to include information that identifies at least one particular individual. For example, in response to a first value of the calculated convolution, Step 1304 may determine that the field is likely to include information that identifies at least one particular individual, and in response to a second value of the calculated convolution, Step 1304 may determine that the field is not likely to include information that identifies at least one particular individual. In some examples, Step 1304 may analyze one or more pixels of the at least part of the one or more images to generate a transformed image, and may use the transformed image to determine whether the field is likely to include information that identifies at least one particular individual. For example, in response to a first transformed image, Step 1304 may determine that the field is likely to include information that identifies at least one particular individual, and in response to a second transformed image, Step 1304 may determine that the field is not likely to include information that identifies at least one particular individual.

In some examples, Step 1306 may comprise receiving an access request of a user. In one example, Step 1306 may read the access request from a memory (such as memory units 210, shared memory modules 410, and so forth). In another example, Step 1306 may receive the access request from an

69

external device over a communication network using a communication device (such as communication modules 230, internal communication modules 440, external communication modules 450, and so forth). In yet another example, Step 1306 may receive the access request from the user (for example, through a user interface, through a web page, using an input device, and so forth).

In some examples, receiving the access request of the user by Step 1306 may comprise accessing a stream of digital communication data sent by a first computing device to a second computing device, and analyzing the stream to detect the request in the stream, for example using a pattern matching algorithm, by parsing a protocol used for communication over the stream, and so forth. In one example, the analysis of the stream may be performed by a third computing device, the third computing device may differ from the first computing device and from the second computing device. In another example, the analysis of the stream may be performed by the second computing device. In yet another example, the analysis of the stream may be performed by the first computing device. In one example, the second computing device may be configured to access the at least part of the content of the field in the data collection in response to the access request of the user. In one example, the stream of digital communication data may be accessed by a privacy firewall, for example as described above. In another example, the stream of digital communication data may be read from a memory (such as memory units 210, shared memory modules 410, and so forth), may be received from an external device over a communication network using a communication device (such as communication modules 230, internal communication modules 440, external communication modules 450, and so forth), may be received from a communication network using network sniffing techniques, and so forth.

In some examples, Step 1308 may comprise accessing a permission record associated with the user of Step 1306. For example Step 1308 may access the permission record in a memory (such as memory units 210, shared memory modules 410, and so forth). In another example, Step 1308 may access the permission record at an external device over a communication network using a communication device (such as communication modules 230, internal communication modules 440, external communication modules 450, and so forth). In yet another example, Step 1308 may access the permission record in permissions 716. For example, the permission record may include an indication of a permission corresponding to the user (or a group of users that including the user) and the data collection of Step 1302. Other examples are described above, for example with relation to permissions 716. In some examples, values in the permission record may include at least one of a permission corresponding to the user of Step 1306 and the data collections of Step 1302 (such as 'read only', 'edit', etc.), a type of the permission (such as 'temporary', 'permanent', etc.), and so forth.

In some examples, Step 1310 may comprise, for example in response to a determination by Step 1304 that the field identified by Step 1302 as a repeated field is likely to include information that identifies at least one particular individual and a first value in the permission record accessed by Step 1308, denying access of the user of Step 1306 to at least part of the content of the field in the data collection of Step 1302. In some examples, Step 1312 may comprise, for example in response to a determination by Step 1304 that the field identified by Step 1302 as a repeated field is not likely to include information that identifies at least one particular

70

individual and the first value in the permission record accessed by Step 1308, providing access of the user of Step 1306 to the at least part of the content of the field in the data collection of Step 1302. In some examples, Step 1314, for example in response to a second value in the permission record accessed by Step 1308, providing access of the user of Step 1306 to the at least part of the content of the field in the data collection of Step 1302.

In some examples, the content of the field in the data collection may be used to generate a de-identified copy of the field. For example, the content of the field in the data collection may be analyzed using pseudonymization or k-anonymization algorithms to generate the de-identified copy of the field. Further, in some examples, for example in response to a determination by Step 1304 that the field identified by Step 1302 as a repeated field is likely to include information that identifies at least one particular individual and the first value in the permission record, method 1300 may provide access to content of the generated de-identified copy of the field.

It will also be understood that the system according to the invention may be a suitably programmed computer, the computer including at least a processing unit and a memory unit. For example, the computer program can be loaded onto the memory unit and can be executed by the processing unit. Likewise, the invention contemplates a software program being readable by a computer for executing the method of the invention. The invention further contemplates a non-transitory computer readable medium storing a software program comprising data and/or computer implementable instruction for carrying out any one or more of the methods described above.

What is claimed is:

1. A non-transitory computer readable medium storing a software program comprising data and computer implementable instructions for carrying out a method for ownership determination, the method comprising:

receiving a request of a user to perform an action for creating a new data collection using one or more source data collections;

accessing one or more ownership records to determine ownership status of the one or more source data collections;

accessing one or more permission records to determine permission status of the user in relation to the one or more source data collections;

in response to a determination that the user does not have permission to view at least part of at least one of the one or more source data collections and that the user is not an owner of the at least one of the one or more source data collections, determining that the user is not an owner of the new data collection;

in response to a determination that for each data collection of the one or more source data collections the user is at least one of an owner of the data collection or has permission to view the entire data collection, determining that the user is an owner of the new data collection; determining an entropy of the data collection of the new data collection;

in response to a first entropy of the new data collection, determine a first permission of the user in relation to the new data collection; and

in response to a second entropy of the new data collection, determine a second permission of the user in relation to the new data collection, the second permission differs from the first permission.

71

2. The non-transitory computer readable medium of claim 1, wherein receiving the request of the user comprises:
accessing a stream of digital communication data sent by
a first computing device to a second computing device;
and

analyzing the stream to detect the request in the stream.

3. The non-transitory computer readable medium of claim 2, wherein the second computing device is configured to perform the action for creating the new data collection using the one or more source data collections in response to the request of the user.

4. The non-transitory computer readable medium of claim 2, wherein the analysis of the stream is performed by a third computing device.

5. The non-transitory computer readable medium of claim 2, wherein the analysis of the stream is performed by the second computing device.

6. The non-transitory computer readable medium of claim 1, wherein the method further comprises performing the action for creating the new data collection using the one or more source data collections.

7. The non-transitory computer readable medium of claim 1, wherein the action for creating the new data collection using the one or more source data collections comprises selecting a parameter for optimizing a function of data included in the one or more source data collections.

8. The non-transitory computer readable medium of claim 1, wherein the action for creating the new data collection using the one or more source data collections comprises calculating a value of a function of data included in the one or more source data collections.

9. The non-transitory computer readable medium of claim 1, wherein the action for creating the new data collection using the one or more source data collections comprises calculating a gradient of a function of data included in the one or more source data collections.

10. The non-transitory computer readable medium of claim 1, wherein the action for creating the new data collection using the one or more source data collections comprises calculating a statistical measurement of data included in the one or more source data collections.

11. The non-transitory computer readable medium of claim 1, wherein the one or more source data collections includes a plurality of records, the action for creating the new data collection using the one or more source data collections comprises training a machine learning model using a first portion of the plurality of records, and the new data collection includes at least a prediction of the trained machine learning model for at least one record of the plurality of records not included in the first portion of the plurality of records.

12. The non-transitory computer readable medium of claim 1, wherein the method further comprises determining at least one owner of the new data collection based on the determined ownership status of the one or more source data collections, the at least one owner do not include the user.

13. The non-transitory computer readable medium of claim 1, wherein the method further comprises determining at least one owner of the new data collection based on the determined ownership status of the one or more source data collections and on the determined permission status of the user in relation to the one or more source data collections, the at least one owner do not include the user.

14. The non-transitory computer readable medium of claim 1, wherein the method further comprises, in response to a determination that the user does not have permission to

72

use at least part of the one or more source data collections to create different data collections, denying the request.

15. The non-transitory computer readable medium of claim 1, wherein the method further comprises updating the one or more ownership records based on the determination of whether the user is an owner of the new data collection.

16. The non-transitory computer readable medium of claim 1, wherein the method further comprises updating the one or more permission records based on the determination of whether the user is an owner of the new data collection.

17. The non-transitory computer readable medium of claim 1, wherein the method further comprises updating the one or more permission records based on the determined permission status of the user in relation to the one or more source data collections.

18. A system for ownership determination, the system comprising:

at least one processing unit configured to:

receive a request of a user to perform an action for creating a new data collection using one or more source data collections;

access one or more ownership records to determine ownership status of the one or more source data collections;

access one or more permission records to determine permission status of the user in relation to the one or more source data collections;

in response to a determination that the user does not have permission to view at least part of at least one of the one or more source data collections and that the user is not an owner of the at least one of the one or more source data collections, determine that the user is not an owner of the new data collection;

in response to a determination that for each data collection of the one or more source data collections the user is at least one of an owner of the data collection or has permission to view the entire data collection, determine that the user is an owner of the new data collection; determining an entropy of the data collection of the new data collection;

in response to a first entropy of the new data collection, determine a first permission of the user in relation to the new data collection, and

in response to a second entropy of the new data collection, determine a second permission of the user in relation to the new data collection, the second permission differs from the first permission.

19. A method for ownership determination, the method comprising:

receiving a request of a user to perform an action for creating a new data collection using one or more source data collections;

accessing one or more ownership records to determine ownership status of the one or more source data collections;

accessing one or more permission records to determine permission status of the user in relation to the one or more source data collections;

in response to a determination that the user does not have permission to view at least part of at least one of the one or more source data collections and that the user is not an owner of the at least one of the one or more source data collections, determining that the user is not an owner of the new data collection;

in response to a determination that for each data collection of the one or more source data collections the user is at least one of an owner of the data collection or has

73

permission to view the entire data collection, determining that the user is an owner of the new data collection; determining an entropy of the data collection of the new data collection;
in response to a first entropy of the new data collection, 5
determine a first permission of the user in relation to the new data collection; and
in response to a second entropy of the new data collection, determine a second permission of the user in relation to the new data collection, the second permission differs 10
from the first permission.

* * * * *

74